INFLUENCING AND EXPLOITING BEHAVIORAL NORMS IN CYBERSPACE TO PROMOTE ETHICAL AND MORAL CONDUCT OF CYBERWARFARE

BY

LT COL GLEN R. SHILLAND

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2010

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

MAJOR IAN B. W. BRYAN (Date)

JOHN B. SHELDON, PhD (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant Colonel Glen Shilland graduated from the University of Michigan with a Bachelor of Science in Aerospace Engineering in 1992. He entered the Air Force a year later as a distinguished graduate of Officer Training School. His first assignment was with the 1st Space Operations Squadron at Falcon AFB, CO as a satellite operations officer where he performed command and control for launch, early orbit, and station keeping on: DSP, DMSP, GPS, and TAOS spacecraft. He attended Undergraduate Navigator Training at Pensacola NAS, FL and transitioned to the flying world as a navigator on the B-52H with the 23rd Bomb Squadron in Minot, ND. After upgrading to Radar Navigator (bombardier) and earning distinguished graduate honors at Squadron Officer School, he volunteered to be an Air Liaison Officer and was a distinguished graduate of the Joint Firepower Control Course.

He deployed with the 5th Special Forces Group during the first days of Operation IRAQI FREEDOM, for which he was awarded a Bronze Star. He has also been deployed as Director of Operations with the 19th Air Support Operations Squadron in the 101st Airborne Division Headquarters, Mosul, Iraq, after which he returned to flying as an instructor and flight commander. His most recent deployment was as Assistant Director of Operations with the 23rd Expeditionary Bomb Squadron in support of Operation ENDURING FREEDOM, flying 327 combat hours out of Diego Garcia, BIOT, where he earned an award as the 8th Air Force Operational Warrior Navigator of the Year.

Lieutenant Colonel Shilland holds Master degrees in Environmental Policy and Management from the University of Denver and in Operations Research from the Air Force Institute of Technology. He recently completed studies at the School of Advanced Air and Space Studies, and will become the Branch Chief for Strategic Plans in Global Strike Command at Barksdale AFB, LA in July.

ACKNOWLEDGEMENTS

First, a big thanks to all the faculty and students at SAASS, it is no exaggeration to say that everyone contributed an idea, a book suggestion, a comment, or a humiliating kick in the metaphorical kidneys to keep me focused toward the goal of thesis completion and graduation.

Next, to my all-suffering and rarely complaining family I owe a debt of gratitude that it is impossible to repay. Thank you for putting up with a grumpy husband, bad dad, and sleepy participant in your lives—you are in my heart always.

Also, to the wonderful people at Google whose policy of “transparency, choice, and control” basically describes my recommendation for norms of behavior; I could not have completed this project without your search engine—keep up the good work.

A special thank you to the legal experts—Colonel Gary Brown, Colonel Guillermo Carranza, and Major Ian Bryan—who helped to balance my thoughts on the scales of justice; this is a much better product as a result of your work.

Finally, to the world and God, thank you for keeping my life interesting.

ABSTRACT

The United States military is committed to conduct warfare within certain ethical and moral limits, generally defined by the law of armed conflict and other domestic and international laws. The law of armed conflict is the product of centuries of custom, treaties, and reciprocity in warfare and it provides a basis for the limits of cyberwarfare. However, applying these limits in cyberspace is complicated, because actors are notoriously anonymous, civilian and military infrastructure is intertwined, cyber sovereignty has not been defined, and assessing the impact of cyberattacks is exceedingly difficult. This paper explores the interaction of the principles of the law of armed conflict —military necessity, humanity, proportionality, distinction, chivalry, and neutrality— with cyberspace behavioral norms—access and connectivity, trust and security, privacy and anonymity, monitoring and control—and suggests avenues to influence and exploit these norms to facilitate ethical and moral conduct of cyberwarfare.

CONTENTS

Introduction

> *Countries or individuals that engage in cyber attacks should face consequences and international condemnation.... We can create norms of behavior among states and encourage respect for the global networked commons.*
>
> -- *United States Secretary of State Hillary Rodham Clinton*

An Army specialist smiles past a cigarette and points suggestively at a naked, hooded prisoner standing on cold, wet, cement ... or smiles past the same cigarette while standing arm in arm with two children in front of a newly built school.

An Air Force missile from a remotely piloted drone slams into a baked clay hovel on the edge of nowhere, burying a frightened family of four ... or the same family is the recipient of humanitarian aid delivered by tactical airlift.

Marines conducting a night raid detain three individuals who are later released only to become insurgents based on their experience ... or the removal of their oppressive presence liberates others to support a worthy cause.

A Navy cruiser detects, tracks, and destroys a civilian airliner with automatic systems designed for safety and efficiency ... or snipers on the stern of a destroyer kill three pirates simultaneously to free hostages with no collateral damage.

These are iconic images of a military that prides itself on adhering to the law of armed conflict (LOAC). These are stories told and retold by a global media and community with instant universal access to information. These are examples of how perceived moral and ethical conduct in warfare alters the capacity to affect events and influence norms of behavior—positively or negatively.

Acting within moral and legal restraints helps sustain domestic and international legitimacy. As conflict moves into cyberspace and public reaction to global effects becomes instantaneous, it will be even more important to maintain this perception of legitimacy. Since morality and ethics follow socially accepted norms of behavior, cultivating norms to enable or constrain freedom of action in cyberspace becomes a matter of national security. Throughout history great powers have shaped norms of behavior to benefit their interests—through diplomacy, information campaigns, military force, and economics. This paper will discuss the methods and merits of influencing and exploiting cyberspace norms to limit conduct of cyberwarfare within LOAC.

Morality and Ethics on the World Stage

Mass media has always been a format for manipulating public opinion and influencing decisions. In a letter to John Jay in 1786, Thomas Jefferson wrote, "Our liberty cannot be guarded but by the freedom of the press, nor that be limited without danger of losing it."[1] Our founding fathers understood the significance of an informed populace and the power of words to inflame popular passions. While the ideal for the media is to present a broad-based, open access to facts and events, mass media is often used "as a systematic form of purposeful persuasion that attempts to influence the emotions, attitudes, opinions, and actions of specified target audiences for ideological, political, or commercial purposes."[2] This is also the definition of propaganda.

Propaganda has only taken on a negative connotation after it was used in the early twentieth century to incite political, racist, and ideological fervor. Throughout history, however, people have employed the most effective propaganda means available to sway public opinion. Orators from Pericles to Obama have inspired nations with rhetorical visions of grandeur, and Gutenberg's invention provided a platform for propaganda unrivaled until the introduction of radio. In 1980, Ted Turner started the first 24-hour television news program, and the Internet has elevated the availability of up-to-the-second personalized information to unparalleled heights. Politicians, businessmen, journalists, and citizens worldwide recognize that these mediums are used to spread messages to explain, justify, condemn, or undermine actions taken on the world stage.

As Michael Walzer states in *Just and Unjust Wars*, "Strategy, like morality, is a language of justification."[3] Nations use moral and legal justification as part of a strategy to build legitimacy on the domestic front and in the international community. While many scholars argue that justification is unnecessary if one has the power to enforce one's will, there are consequences for violating generally accepted norms of behavior in

[1] Thomas Jefferson to John Jay, letter, 1786 quoted in University of Virginia, *Jeffersonian Cyclopedia*, ed. John Foley (New York, NY: Funk & Wagnalls, 1900), no. 4702. Found in Jefferson Digital Archive http://etext.virginia.edu/etcbin/foley-page?id=JCE4702 (accessed 22 February 2010).

[2] Richard Alan Nelson, *A Chronology and Glossary of Propaganda in the United States* (Westport, CT: Greenwood Press, 1996), 232.

[3] Michael Walzer, *Just and Unjust Wars* 4th ed. (New York, NY: Basic Books, 2006), 13.

diplomacy, business, journalism, and warfare.[4] Acting within a mutually acceptable set of moral and legal justifications for warfare allows individuals and groups to pursue their interests legitimately.

Today's information warfare goes beyond mere manipulation of opinion however. Cyberattacks can destroy, degrade, disrupt, deny, and deceive information systems almost as easily as kinetic attacks. It is debatable whether a true cyberwar has occurred, but operations in Estonia, Georgia, Korea, Taiwan, and around the world have tested the limits of justifiable behavior in cyberspace. The law of armed conflict (LOAC) has evolved over centuries of warfare and guides the United States' actions in cyberspace, but application can be problematic under the best circumstances.[5] Current norms of behavior can complicate the utility of LOAC in cyberwarfare and blur the lines of what constitutes an act of war.

War's moral limitations can be expressed at two levels, *jus ad bellum*—the right to engage in war, and *jus in bello*—the proper conduct within war. Libraries have been written on these subjects, and this paper cannot begin to explore the psychosocial intricacies of their universal application. The focus of this thesis is how the United States can shape norms of behavior to strengthen *jus in bello* in cyberspace. The first chapter will provide a brief overview of the history of LOAC, its principles, its application in international law, and the major international conventions pertaining to armed conflict. Chapter three will investigate how LOAC can be applied to cyberwarfare.

The Nature of War is Immutable

In a much underappreciated work, *Military Strategy: A General Theory of Power Control*, Rear Admiral J. C. Wylie outlined four basic assumptions underlying a general theory of war: despite whatever effort there may be to prevent it, there may be war; the aim of war is some measure of control over the enemy; we cannot predict with certainty the pattern of the war for which we prepare ourselves; and the ultimate determinant in

[4] Followers of the realist school have long argued that "the strong do what they can and the weak suffer what they must" but the existence of criminal and civil domestic and international law indicates that there are generally accepted rules of behavior outside of which people act at their own risk.

[5] Based on comments by Air Force General Kevin P. Chilton, quoted in Jeff Schogol, "Official: No Options 'Off the Table' for U.S. Response to Cyber Attacks," *Stars and Stripes*, 8 May 2009, http://www.stripes.com/article.asp?section=104&article=62555 (accessed 26 March 2010); Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 30.

war is the man on the scene with the gun.[6] He described war as a collapse rather than a continuation of policy; refuting Carl von Clausewitz' famous aphorism. However, there are few who would dispute the eternal validity of the Prussian general's trinity of war—the violent passions of the people, the fog and friction experienced by the commander and his army, and the government's rational pursuit of policy. Regardless of the environment or circumstances, writes Clausewitz, war will follow these basic tendencies "like an object suspended between three magnets."[7] Cyberspace will not change the fundamental nature of warfare; it will simply be another domain in which people, commanders, and governments fight for national advantage using traditional tools of international politics.[8]

As Robert Gilpin explains, "in the beginning of the twenty-first century, the battleground has been located among the high-tech industries of the computer and the information economies."[9] While academics debate whether war can be violent without inflicting physical damage, or without involving governments, or if a cyber domain even exists, the fact that nation-states and their subgroups are attempting to exert control through the use of cyberspace is irrefutable. Control of information has been contested since the first road was built; conflict on the information superhighway is merely the contest's latest venue. To paraphrase and adapt Julian Corbett's maritime strategy, command of cyberspace, therefore, means nothing but the control of cyber communications, whether for commercial or military purposes.[10] Assuming war will happen, cyberspace will be used as both a domain and an instrument of war, and we must be prepared to exert control over the environment. The technical details of how this is accomplished and for what purpose, are irrelevant to a discussion on the moral conduct of war within cyberspace.

[6] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1967), 66-72.
[7] Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1976), 89.
[8] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York, NY: Oxford University Press, 2006), 165.
[9] Robert Gilpin, *Global Political Economy* (Princeton, NJ: Princeton University Press, 2001), 140.
[10] The actual statement is: "Command of the sea, therefore, means nothing but the control of maritime communications, whether for commercial or military purposes." from Julian S. Corbett, *Some Principles of Maritime Strategy*, (London, England: Longmans, Green & Co., 1911), 94.

Franklin Kramer remarks there are at least 28 different definitions of cyberspace, but the one used for this paper was published in the Quadrennial Defense Review Report of February 2010: cyberspace—a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks.[11] Regardless of how it is defined, "an increasingly wide range of social, political, economic, and military activities are dependent on it and thus are vulnerable to both interruption of its use and usurpation of its capabilities."[12] Since conflict is inevitable in cyberspace due to its value and vulnerability, the United States must determine how to fight within the moral, legal, and physical limitations imposed on and by the domain.

While the nature of war may not change, the nature of the cyberspace domain poses unique challenges for determining and containing the effects of cyberwarfare. James Lewis states, "Uncertainty is the most prominent aspect of cyber conflict—in attribution of the attackers [sic] identity, the scope of collateral damage, and the potential effect on the intended target from cyber attack."[13] Due to the anonymity of actors in cyberspace, the interconnectivity of civilian and military infrastructure and personnel, and the difficulty assessing the impact of cyberattacks from both an offensive and defensive perspective, controlling cyberwarfare can be wickedly complex.[14] Chapter two will discuss the existing cyber law, doctrine, and ethics that frame the paradoxes and dilemmas of cyberwarfare.

[11] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 4; Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 14.

[12] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 24.

[13] James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies, October 2009, http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (accessed 30 October 2009).

[14] Leon Fuerth describes the new order of "wicked" public issues that "involve ceaseless interaction of systems within systems, the constant possibility of surprise, and the primacy of the law of unintended consequences in, "Cyberpower from the Presidential Perspective," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 557. The term "wicked problem" was first introduced in Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences 4*, (1973), 155-169.

Behavioral Norms and Cyberwarfare are Interconnected

Arguably the most critical phase of warfare happens before armed conflict begins, as explained by Sun Tzu: “Those skilled in war bring the enemy to the field of battle and are not brought there by him.”[15] Influencing and exploiting norms of behavior will be decisive in preparing the cyberspace battlefield, and those skilled in the art of war will prepare the battlefield to their advantage. According to the unabridged Oxford dictionary, a *norm* can be “an ideal standard binding upon the members of a group and serving to guide, control, or regulate proper and acceptable behavior,” or “a pattern or trait taken or estimated to be typical in the behavior of a social group because [it is] most frequently observed.” The subtle difference between an *ideal* and a *pattern* is the difference between what *should* be and what *is*. The ideals embodied in the law of armed conflict will be constrained by the patterns of behavior that develop in cyberspace, which are supported by society and ultimately enforced by government coercion.

For instance, the perceived expectation of anonymity and privacy while online has grown into an abiding norm of cyberspace behavior. This norm conflicts with the LOAC principle of target discrimination, because of the near impossibility to accurately attribute an attack to a responsible civilian or military entity. Thus, either the norm or the law has to change to accommodate reality. This is one of the many problems nation-states face in prescribing limitations to cyberwarfare. In the words of one legal scholar, “One result of any eventual [Information Warfare] law will be to provide military officers with a clear understanding of when the use of [Information Warfare] is legally acceptable and how those attacks should be conducted and targeted to avoid violating LOAC principles.”[16]

Determining how to apply LOAC in cyberspace is only the start of the problem. Social and physical limitations regulating cyber activity may dictate the boundaries of possibility for cyberwarfare, but they can also be altered based on our expectations. When cyberspace was first envisioned, “many believed that international standards applied to the Internet could eliminate the parochialism of territorial legalism.”[17] Internet idealists anticipated the end of nationalism and the rise of global governance. Others

[15] Sun Tzu, *The Illustrated Art of War*, ed. and trans. by Samuel B. Griffith (Oxford, England: Oxford University Press, 2005), 6.2, 145.
[16] Jon P. Jurich, “Cyberwar and Customary International Law,” *Chicago Journal of International Law 9*, no. 1 (Summer 2008): 275-294.
[17] Goldsmith and Wu, *Who Controls the Internet?*, 27.

perceived the birth of a new liberal world order—one that depended on an "Internet Common Law" based on the social norms of a cyberspace community rather than on traditional international law.[18] Defining norms of behavior in cyberspace was seen as a means to change the nature of governance and perhaps even society itself.

Over a quarter-century later, the nation-state survives, history has not ended, and the world is not flat. One reason is that nation-states have only just begun to assert their sovereignty in cyberspace, national doctrine for cyberspace is still being written, and the limits of power in cyberspace have yet to be discovered. Another reason is that cyberwarfare has not manifested itself completely, cyber law is still in its formative years, and the norms of cyberspace behavior have not been fully identified or developed. Chapter four will detail what the United States can do globally to influence these norms, and the paper will conclude with a broad strategy for control of cyberspace.

[18] Marcelo Halpern and Ajay K. Mehrota, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age," *University of Pennsylvania Journal of International Economic Law 21,* (Fall 2007): 523-561.

Chapter 1

Moral and Legal Limitations of Warfare

> *Attached to force are certain self-imposed, imperceptible limitations hardly worth mentioning, known as international law and custom, but they scarcely weaken it.*
>
> -- *Carl von Clausewitz*

The venerable strategist harbored disdain for international legal restrictions, and would have agreed that "restraints on war grew out of the cultures of war-making societies, rather than being imposed on them by some transcendent moral order."[1] However, while disparate cultures have developed unique concepts of warfare due to variation in a multitude of factors including secular and religious values, geography, technology, business practices, and political concerns, they all recognize that certain actions are manifestly wrong. Michael Walzer contends that "war is a social creation. The rules actually observed or violated in this or that time and place are necessarily a complex product," but he also states that some rules are "more closely connected to universal notions of right and wrong."[2]

Non-Western cultures have developed their own principles for law and warfare, most prominently Islamic Shar'ia and Chinese Confucianism. Although their sources are different, the concept of limiting violence to combatants as much as possible remains constant. The Qur'an for instance says, "Fight in the cause of Allah those who fight you, but do not transgress limits; for Allah loveth not transgressors" (2:190). For Muslims, the Qur'an is the ultimate arbiter of law, but in Confucianism, "rule of law is considered a state of barbaric primitiveness, prior to achieving the civilized state of voluntary observation of proper rites."[3] In fact, Confucians are strongly in favor of openness and fair play in war, though its practitioners rely on hierarchical loyalty rather than codified

[1] Michael Howard, "Constraints on Warfare," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 2.

[2] Michael Walzer, *Just and Unjust Wars* 4th ed. (New York, NY: Basic Books, 2006), 42-3.

[3] Henry C. K. Liu, "China—The Abduction of Modernity—Part 3: Rule of Law vs. Confucianism," *Asia Times*, 24 July 2003, http://www.atimes.com/atimes/China/EG24Ad01.html (accessed 22 March 2010).

law.[4] Whether modern adherents to these codes actually follow their underlying ideals is irrelevant as long as they are generally accepted as legitimate. Regardless of whether people perceive the world as being in a state of perpetual conflict or harmony, certain restrictions are universally acknowledged in the conduct of war.

Despite the historical malleability and cultural interpretations of morality in war, it has generally been accepted since at least the nineteenth century that "populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience."[5] The moral and legal limitations of warfare have evolved through centuries of custom during quarrels over land, sea, air, and space, and they are codified in a multitude of treaties and conventions, which are sustained by international reciprocity. However, while its principles are generally respected worldwide, the law of armed conflict (LOAC) primarily grew out of Western concepts of morality and legality.

Western Principles of Morality in Warfare and the Law of Armed Conflict

The concepts of just war—*jus ad bellum*, and proper conduct of war—*jus in bello*, "have largely been shaped by Christian ethic defined by leading teachers in the Catholic church of the Middle Ages and the Renaissance."[6] In fact, the Western laws of war rest upon the same five foundations: the Bible (above all Deut. 20:10-20), Roman law, canon law (especially the *Decretum* of Gratian [*Concordia discordantium canonum*]), the writings of Augustine, and the *Summae* of Thomas Aquinas.[7] These works characterized the essential limits of moral and legal conduct in human affairs, which were then applied specifically to warfare. "However," states Geoffrey Parker, "this powerful combination of natural and divine law, ecclesiastical precept, military law, common custom, and self-

[4] Stephen C. Neff, *War and the Law of Nations* (Cambridge, England: Cambridge University Press, 2005), 22.

[5] Hague Conference, *Convention with Respect to the Laws and Customs of War on Land (Hague II)*, 29 July 1899, preamble.

[6] Howard, "Constraints on Warfare," 2.

[7] Geoffrey Parker, "Early Modern Europe," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 41.

interest only coalesced to impart a new and enduring consistency to both the *jus ad bellum* and the *jus in bello* in the period between 1550 and 1700 [AD]."[8]

Before that time, conflict was constrained by customary rules, but these rules did not prohibit massacre, rape, and pillage of the general populace. Josiah Ober points out that "archaic and early classical Greek social mores and political culture supported a form of warfare that was highly, if informally, rule oriented," but their courts sanctioned the slaughter and enslavement of entire city-states such as Platea.[9] By the end of the Peloponnesian war the hoplite structure of warfare had broken down into internecine civil wars without restriction. Likewise, through the Roman era and into the Age of Chivalry (1100-1500 AD) "so long as it was fought for pious ends, such warfare knew no effective limits."[10] However, near the end of the sixteenth century, new restraints on the level of acceptable violence were introduced with the professionalization of armies, the de-emphasis of religion as a cause for war after the Peace of Westphalia in 1648, the escalating destructive capability of the instruments of war, and a steady spread of reciprocity between warring parties, at least in Europe.[11] Major world powers attempted to establish laws unilaterally through institutions like Great Britain's High Court of the Admiralty, or multilaterally through declarations such as those of Paris in 1856 and St. Petersburg in 1868, but it took more than three centuries for customs to be codified into a system of universally applicable laws at The Hague in 1899 and 1907 and at Geneva in 1949.

In addition to religious and cultural limitations, there are two major schools of Western secular philosophical thought on morality in war: absolutism and utilitarianism. As Thomas Nagel explains, "An absolutist can be expected to try to maximize good and minimize evil, so long as this does not require him to transgress an absolute prohibition like that against murder. But when such a conflict occurs, the prohibition takes complete

[8] Parker, "Early Modern Europe," 42.

[9] Customs guided activities such as truces, alliances, the proper treatment of prisoners and noncombatants, and removal of the dead. Josiah Ober, "Classical Greek Times," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 13, 25; Robert B. Strassler, *The Landmark Thucydides* (New York, NY: Simon & Schuster, 1996), 3.68.

[10] Robert C. Stacey, "Age of Chivalry," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 28.

[11] Parker, "Early Modern Europe," 53-55.

precedence over any consideration of consequences."[12] A utilitarian on the other hand does not accept absolute prohibitions, but chooses the lesser of two (or more) evils when confronted with a moral conflict in an attempt to maximize long-range utility following rational rules.[13] Most leaders follow a utilitarian policy, because in order to survive they must learn how to do wrong, as Machiavelli cautions in *The Prince*. Michael Walzer is credited with defining this as the "dirty hands dilemma"—the inability of politicians to act effectively without compromising their ideals.[14]

Utilitarianism dominates LOAC. Those who engage in warfare acknowledge that some measure of death and destruction is inevitable; the danger to humanity is that the carnage will escalate without bounds. The goal of LOAC is to reduce the violence to only that which is minimally necessary to subdue the enemy, while sparing those who are not party to the conflict. Whether our enemies fight according to these principles or not, we recognize that "America must align its ethical principles with the nation's strategic requirements."[15] To meet its strategic goals legitimately on both the domestic and international stage, the United States must not only ensure its wars are justified—*jus ad bellum*—but, perhaps most importantly, ensure that it fights justifiably—*jus in bello*. The principal tenets of *jus in bello* as defined in LOAC and by the U.S. Army Operational Law Handbook are: military necessity, humanity, proportionality, and distinction.[16] Chivalry and neutrality are also commonly accepted principles.

Military Necessity

The Air Force defines military necessity as "only that degree of regulated force, not otherwise prohibited by the laws of war, required for the partial or complete submission of the enemy with the least expenditure of life, time, and physical

[12] Thomas Nagel, "War and Massacre," in *War and Moral Responsibility*, ed. Marshall Cohen, Thomas Nagel, and Thomas Scanlon (Princeton, NJ: Princeton University Press, 1974), 8.

[13] R. B. Brandt, "Utilitarianism and the Rules of War," in *War and Moral Responsibility*, 30.

[14] Machiavelli is the ultimate pessimistic realist as he warns readers that "he who neglects what is done for what ought to be done, sooner effects his ruin than his preservation; for a man who wishes to act entirely up to his professions of virtue soon meets with what destroys him among so much that is evil." Walzer concurs that while politicians want to act idealistically, they are unable to attain and maintain power without associating with unsavory characters and compromising their idealistic goals to some extent. Nicolo Machiavelli, *The Prince*, trans. W. K. Marriott (Rockville, MD: Arc Manor, 2007), Chapter XV; Michael Walzer, "Political Action: The Problem of Dirty Hands," in *War and Moral Responsibility*, 66.

[15] Sarah Sewell, *Introduction to the U.S. Army and Marine Corps Counterinsurgency Field Manual* (Chicago, IL: The University of Chicago Press, 2007), xxii.

[16] International and Operational Law Department, *Operational Law Handbook* (Charlottesville, VA: U.S. Army Judge Advocate General School, 2003), 8-10.

resources."[17] This principle can also be related to economy of force because attacking anything other than a military objective can be considered a waste of resources. The Geneva Conventions define military objectives as "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[18] Thus military necessity calls for the measured use of force against objectives that are being actively used for military purposes, or can legitimately be considered useful for future military advantage.

The Geneva Conventions invoke the use of military necessity multiple times, including the prohibition of "willful killing, torture or inhuman treatment, including biological experiments, willfully causing great suffering or serious injury to body or health, and extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."[19] The Conventions also protect "real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations."[20] Specific protection is given to "works or installations containing dangerous forces, namely dams, dykes [sic] and nuclear electrical generating stations," unless they are in "regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support."[21] In all military operations, the primary concern behind military necessity is to ensure that "constant care shall be taken to spare the civilian population, civilians and civilian objects."[22]

Humanity

To reinforce the reduction of suffering, LOAC also contains specific prohibitions on the allowable instruments of war to demonstrate that "the right of belligerents to adopt

[17] Judge Advocate General School, *The Military Commander and the Law*, 8th ed. (Maxwell Air Force Base, AL: U.S. Air Force Judge Advocate General's School, 2006), 614.
[18] Geneva Conference, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, Article 52(2).
[19] Geneva Conference, *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949, Article 50.
[20] Geneva Conference, *Convention (IV) Relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, Article 53.
[21] Geneva Conference, *Protocol I*, Article 56.
[22] Geneva Conference, *Protocol I*, Article 57.

means of injuring the enemy is not unlimited."[23] The Hague Conventions prohibit: the employment of poison or poisoned arms; killing or wounding an enemy who, having laid down arms, or having no longer means of defense, has surrendered at discretion; and arms, projectiles, or material of a nature to cause superfluous injury.[24] Nations have also tried to eliminate certain weapons which were considered particularly abominable, such as explosive or incendiary projectiles weighing less than 400 grams; gas-filled projectiles; and hollow-point or soft projectiles which expand or flatten easily in the human body.[25] The Geneva Conventional Weapons Convention of 1980 prohibits fragmentary weapons which can escape detection by X-rays, and certain mines, booby-traps, and incendiary weapons.[26] A final example of this type of limitation is the 1993 Chemical Weapons Convention which outlaws all use of chemical weapons, including for self-defense.[27]

Humanity encompasses not only the weapons used, but the way in which they are employed, specifically to prevent atrocities recurrent in unlimited conflicts. Common Article 3 of the Geneva Conventions of 1949 decries "murder of all kinds, mutilation, cruel treatment and torture." The Geneva Conventions also established universal guidelines for the ethical treatment of wounded, sick or shipwrecked combatants, prisoners of war, and civilians. Though it is debatable how effective these and other conventions and declarations have been in various conflicts, the clear intent of the international community has been to avoid unnecessary suffering of both belligerents and noncombatants during the conduct of war by restricting the definition and use of legally available weaponry.

Proportionality

In addition to limiting how and what weapons are used, LOAC attempts to prevent the *superfluous* use of allowable weaponry. For instance, an indiscriminate

[23] Hague Conference, *Hague II*, Article 22.
[24] Hague Conference, *Hague II*, Article 23.
[25] Declaration of St. Petersburg, *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, 11 December 1868; and Hague Conference, *Regulations Respecting the Laws and Customs of War on Land (Hague II)*, 29 July 1899, Declarations II and III.
[26] Geneva Conference, *Convention on Prohibitions of Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*, 10 October 1980, Protocols I-III.
[27] Judge Advocate General School, *Military Commander and the Law*, 617.

attack is defined as one “which would be excessive in relation to the concrete and direct military advantage anticipated,” and indiscriminate reprisals against civilians are specifically prohibited.[28] Though this tenet accepts the possibility of collateral damage, a good-faith effort must be made to “take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects.”[29] In practice this becomes a calculation of costs and benefits to the military commander, taking into account the nature of the threat, available weaponry, and potential for unintended consequences.

This principle also appears in the doctrine of double effect. Typically credited to Thomas Aquinas’ discussion of self-defense in his *Summa Theologica*, the argument is that “it is permissible to bring about as a merely foreseen side effect a harmful event that it would be impermissible to bring about intentionally.”[30] The primary question is the *intent* of the actor, with the objective that the harm is only incidental and not essential to producing a necessary effect. In other words, the ends do not justify the means, but bad results can be justified if due diligence is taken to avoid them. A familiar example of double effect is the morally *defensible* act of precision strategic bombing—with the intent of destroying an industrial network difference—as opposed to the morally *reprehensible* act of area (terror) bombing—with the primary intent of destroying a population’s morale.

While LOAC does not specifically address the element of double effect, it implies that “if saving civilian lives means risking soldier’s lives, the risk must be accepted. But there is a limit to the risks that we require.... We can only ask soldiers to minimize the dangers they impose.”[31] In judging a combatant’s action, therefore, one must assess each individual situation to determine if reasonable care has been taken to avoid unnecessary damage based on the information and time available for a decision, while measuring the military advantage gained from the proportional employment of force. This principle is only possible if there is a clear distinction between combatants and noncombatants.

[28] Geneva Conference, *Protocol I*, Article 51, Paragraphs 5(b) and 6.
[29] Geneva Conference, *Protocol I*, Article 57, Paragraph 2(a)ii.
[30] Stanford Encyclopedia of Philosophy, *Doctrine of Double Effect*, 29 June 2009, http://plato.stanford.edu/entries/double-effect/ (accessed 22 March 2010).
[31] Walzer, *Just and Unjust Wars*, 156.

Distinction

This principle is usually applied in reference to the requirement for *aggressors* to differentiate between combatants and noncombatants when applying force; however, to remain within international law *all* participants are obliged to separate military forces from the civilian populace to the greatest extent possible. For instance, the Geneva Conventions state, "Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives."[32] Signatories are also held responsible to ensure that "medical establishments and units are, as far as possible, situated in such a manner that attacks against military objectives cannot imperil their safety."[33] Most importantly, "the presence of a protected person may not be used to render certain points or areas immune from military operations."[34] This precludes the use of so-called human shields to defend otherwise legal military objectives, and puts the onus on the *defender* to identify and separate noncombatants from zones of conflict. This is an important aspect of distinction which is often forgotten by the public.

Some authors contend that the difficulty of distinction is the reason "regular armed services intensely dislike counterinsurgency warfare, fighting opponents who can't be distinguished from local civilians and who may use indiscriminate acts of violence to achieve their political ends."[35] A similar situation is encountered in cyberwarfare, since there is currently no way to distinguish between civilian and military personnel, though some argue that "in cyberwarfare, it seems, there may be no room for noncombatants."[36] Nevertheless, according to international law, all belligerents are held accountable for the safety and security of noncombatants and civilian property, and must make a concerted effort to separate them from legitimate military targets both offensively and defensively. Since this is not always possible, collateral damage must be minimized to the greatest extent possible by available intelligence, time, technology, and military necessity.

[32] Geneva Conference, *Protocol I*, Article 48.

[33] Geneva Conference, *Convention I*, Article 19.

[34] Geneva Conference, *Convention IV*, Article 28.

[35] Paul Kennedy and George J. Andreopoulos, "The Laws of War: Some Concluding Reflections," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 215.

[36] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York, NY: Oxford University Press, 2009), 10.

Chivalry

One of the oldest principles of *jus in bello* is chivalry. It started in the medieval age as "*jus militare* ... a body of international knightly custom," and evolved into "the waging of war in accord with well-recognized formalities and courtesies."[37] These customs include protection of noncombatants such as the young, old and helpless, with specific sanctions against treachery and perfidy. The goal of this principle is to promote mutual restraint, because "combatants find it difficult to respect protected persons and objects if experience causes them to believe or suspect that the adversaries are abusing their claim to protection under [LOAC] to gain a military advantage."[38]

The Hague Conventions prohibit: killing or wounding treacherously individuals belonging to the hostile nation or army; killing or wounding an enemy who, having laid down his arms, or having no longer means of defense, has surrendered at discretion; declaring that no quarter will be given; and making improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention.[39] They also expressly forbid pillage and stress the importance of observing the rules of military honor when accepting capitulations.[40] The precepts against perfidy are further extended in the Additional Protocol I of the Geneva Conventions to include: the feigning of an incapacitation by wounds or sickness; the feigning of civilian, non-combatant status; and the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.[41] The obvious intent of these provisions is to prevent the undermining of protected status through the means of deception.

On the other hand, "ruses of war and the employment of measures necessary for obtaining information about the enemy," such as "camouflage, decoys, mock operations and misinformation" are *not* prohibited.[42] These actions are not considered perfidious because they take advantage of an enemy's gullibility without using the enemy's

[37] Stacey, "Age of Chivalry," 31; Judge Advocate General School, *Military Commander and the Law*, 617.
[38] International and Operational Law Department, *Operational Law Handbook*, 20.
[39] Hague Conference, *Hague II*, Article 23. The Geneva Convention referred to in this case is the 22 August 1864 *Convention for the Amelioration of the Condition of the Wounded in Armies in the Field* which established the International Committee on the Red Cross.
[40] Hague Conference, *Hague II*, Articles 35 and 47.
[41] Geneva Conference, *Protocol I*, Article 37.
[42] Hague Conference, *Hague II*, Article 24; Geneva Conference, *Protocol I*, Article 37.

adherence to the law as a shield. This is why "combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack."[43] Otherwise the conflict might quickly devolve to a state of reciprocal retribution without distinction.

Neutrality

The final principle of LOAC respects the territory and rights of nation-states who are not party to the conflict. The rights of neutrality are codified in Hague Convention V, but they are essentially nullified if the nation-state complies with a call to collective security as specified in Article 43 of the United Nations Charter.[44] The Convention prevents the movement or basing of enemy troops, munitions, or supplies through neutral territory; requires the internment of sick, wounded, shipwrecked sailors, grounded airmen, and prisoners of war (unless they are escaped); and forbids recruitment from neutral territory. The Hague Convention allows neutrals to defend their territory and *impartially* provide loans, services, communications, and commercial goods to belligerents, but forfeits neutrality if the state actively participates in hostilities or allows such actions from its territory.

A key aspect of neutrality from a cyberspace perspective is the concentration on *territory*. Nearly every stipulation is predicated on the assumption of clearly demarcated sovereignty, which is logical considering the Conventions dealt with war on land, sea, and air, but it precludes a simple extension to cyberspace where sovereignty is undefined and non-state actors are prevalent. Though a neutral nation-state could theoretically deny the use of computers, servers, or other elements of cyberspace physically resident on sovereign territory, in practice it would be very hard to enforce due to the random nature of internet routing protocols, the proliferation of dual-use communications, and the ubiquitous scourge of anonymity. The application of LOAC to cyberspace will be more fully addressed in Chapter 3.

[43] Geneva Conference, *Protocol I*, Article 44.

[44] Hague Conference, *Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V)*, 18 October 1907; *Charter of the United Nations*, San Fransisco, CA, 24 October 1945, Article 43 states, "All Members of the United Nations, in order to contribute to the maintenance of international peace and security, undertake to make available to the Security Council, on its call and in accordance with a special agreement or agreements, armed forces, assistance, and facilities, including rights of passage, necessary for the purpose of maintaining international peace and security."

Roots of International Law

A brief interlude may be necessary to discuss the roots of law and how it is applied internationally.[45] Law—a system of rules for human behavior—has existed since the beginning of society. In fact, one could say it is the basis for society itself. There are two major forms of domestic law: codified (civil) law and customary (common) law. Essentially the major difference is that civil law is proscribed by a designated legislative authority and adjudicated separately in each case, while common law is based on judicial precedent and socially derived custom. Other specialized forms include religious (such as Islamic Shari'a) and philosophical (such as Confucian) law. Domestic law depends on a set of legitimate institutions for legislation, adjudication, and enforcement.

International law on the other hand has no such authoritative forums. As Kenneth Waltz points out, "National politics is the realm of authority, of administration, and of law. International politics is the realm of power, of struggle, and of accommodation."[46] Despite the pessimism of realists, the United Nations and its subsidiary, the International Court of Justice, are close approximations of responsible international governing bodies. Article 38 of the Statute of the International Court of Justice provides some guidance on the sources of international law:

> a. **international conventions**, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. **international custom**, as evidence of a general practice accepted as law;
>
> c. the **general principles of law** recognized by civilized nations;
>
> d. subject to the provisions of Article 5 [concerning nominations to the Court] **judicial decisions and the teachings of the most highly qualified publicists of the various nations**, as subsidiary means for the determination of rules of law.

However, "decisions of the International Court, unanimously supported resolutions of the General Assembly of the United Nations concerning matters of law, and important multilateral treaties concerned to codify or develop rules of international law, are all lacking the quality to bind states generally. In a sense 'formal sources' do not exist in

[45] Perhaps half of the written works in history have been about law (and religion) so a comprehensive review and annotated bibliography of this subject is beyond the scope of this paper, but a fairly comprehensive account was compiled by Ian Brownlie, *Principles of Public International Law* 7th ed. (Oxford, England: Oxford University Press, 2008).

[46] Kenneth Waltz, *Theory of International Politics* (Boston, MA: McGraw Hill, 1979), 113.

international law. As a substitute, and perhaps an equivalent, there is the principle that the general consent of states creates rules of general application."[47] This explanation by Ian Brownlie suggests that despite the legitimacy of the Hague and Geneva Conventions, the United Nations Charter, and a myriad of unilateral, bilateral, and multilateral treaties, international law as such depends almost entirely on voluntary adherence to customary practices between nation-states rather than the threat of enforcement.

Black's Law Dictionary defines International Law as "the legal principles governing the relationships between nations; more modernly, the law of international relations, embracing not only nations but also such participants as international organizations, multinational corporations, nongovernmental organizations, and even individuals."[48] Although the recent rise of human rights and environmental law has placed increased emphasis on individuals and organizations, the structure of reciprocity is still essentially between nation-states. Therefore "two of the basic principles of the international legal system are that sovereign states are legally equal and independent actors in the world community, and that they generally assume legal obligations only by affirmatively agreeing to do so."[49] While the lack of an effective enforcement institution provokes an anarchic, self-help structure that is closer to Athenian realism than Melian idealism, multilateral treaties and global forums such as the World Trade Organization and the United Nations have become important instruments of international influence.[50]

One arguable exception to the requisite for reciprocity is the concept of *jus cogens* —a mandatory norm of general international law from which no two or more nations may exempt themselves or release one another.[51] Some tenets of international law, such as the 12 nautical mile limit of territorial waters, are so broadly accepted and essential to international relations that they are binding regardless of whether they are recognized by an individual nation-state or international organization. However, these customs have generally been established through centuries of state practice and are based on the

[47] Brownlie, *Principles of Public International Law*, 3.
[48] *Black's Law Dictionary* 7th ed., s.v. "international law," ed. Bryan A. Garner et al. (St. Paul, MN: West Group, 1990), 822.
[49] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, May 1999), 1.
[50] Read the Melian Dialogue in Robert B. Strassler, *The Landmark Thucydides* (New York, NY: Simon & Schuster, 1996), 5.84.1-5.111; for 'self-help' structural realism see Waltz, *Theory of International Politics*.
[51] *Black's Law Dictionary*, s.v. "*jus cogens*," 864.

consensus of a majority of active participants on the international stage. As such they are *de facto* a form of reciprocity and are subject to change by the community as a whole.

Despite the historic propensity towards a "might makes right" environment, the balance of power has generally constrained nation-states enough to allow a system of international coordination and cooperation to evolve. As the Oxford Companion avers, "states and armed forces, with all their virtues and defects in this regard, remain the main mechanism for implementation and enforcement of the laws of war."[52] This system has actually increased the power of the nation-state, because smaller states have gained a platform to exert pressure on larger states without diminishing the ability of major powers to wield substantial authority when required. A similar situation of nation-state predominance is growing in cyberspace, due to the lack of an international system of governance and the reliance on nation-states to enforce domestic and international law. The relative importance of non-state actors to stimulating international cooperation and influencing norms of behavior in cyberspace is developed further in chapter four.

Modern Legal Limitations on Warfare

The law of armed conflict before the nineteenth century weighed predominantly on the conscience and immortal soul of individual combatants rather than on international actors. As discussed earlier, LOAC "did exist, but in a form very different from today: in custom, in broad principles, in national laws and military manuals, and in religious teaching."[53] Limitations on warfare evolved because "professional soldiers knew the value of the laws and customs [for] military self-interest [though] restraints were ignored when military necessity seemed to require it; and when there were radical political, ethnic, religious, or cultural differences between combatants."[54] Though there have been limited agreements and generally accepted practices of warfare throughout history,

[52] *The Oxford Companion to Military History*, s.v. "laws of war," ed. Richard Holmes et al. (Oxford, England: Oxford University Press, 2001), 493-6.

[53] Adam Roberts, "Land Warfare: From Hague to Nuremberg," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 119.

[54] Gunther Rothenberg, "The Age of Napoleon," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Shulman (New Haven, CT: Yale University Press, 1994), 87.

universal codification of conventions on the conduct of armed conflict was not possible until after the World Wars of the twentieth century.

The Oxford Companion to Military History says the "paradox that one of the first areas of international law to be developed was that which concerned war is partly explained by the fact that peaceful relations can often be regulated on an *ad hoc* basis, whereas wars repeatedly pose questions of a general character which cannot be settled at the time by agreement between adversaries, and therefore need to be addressed earlier."[55] The potential for widespread devastation was foreseen prior to the twentieth century's World Wars, and this apocalyptic vision provided a social impetus for change. The rise of globalization built a worldwide platform for international political reconciliation, and the polarized world order established after the World Wars enabled the Western powers to impose a system approaching universal guidance for the conduct of warfare. The major elements of LOAC are the Hague and Geneva Conventions and the United Nations Charter, but these are merely representative of the wider corpus of applicable customs and treaties. As the International Military Tribunal at Nuremburg, established after World War II, said, "This law is not static, but by continual adaptation follows the needs of a changing world."[56]

Hague Conventions

By the end of the nineteenth century, the world had attained a level of economic interconnectivity unparalleled until the Internet. The Industrial Revolution also unleashed powers of destruction and mobilization that dwarfed previous ages. National governments realized the value of a standard method for international arbitration and non-violent conflict resolution, and attempted to codify a platform for disarmament and mediation in the Hague Conventions of 1899 and 1907. They did not eliminate war as a legitimate tool of statecraft, but their efforts led to general acceptance of the Western ideals of *jus ad bellum* and *jus in bello*, and resulted in "the first general codification of laws of land war in the form of a multilateral treaty ever to have been concluded."[57]

[55] *Oxford Companion to Military History*, s.v. "laws of war," 493-6.
[56] Quoted in W. Michael Reisman and Chris T. Antoniou, eds., *The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict* (New York, NY: Vintage Books, 1994), xix.
[57] Roberts, "Land Warfare," 121.

One of the major successes of the peace conferences at The Hague prior to World War I was the establishment of a Permanent Court of Arbitration, which evolved into the International Court of Justice after the establishment of the United Nations.[58] As stated in Article 1 of the first Hague Convention, the object was, "With a view to obviating as far as possible recourse to force in the relations between States, the Contracting Powers agree to use their best efforts to ensure the pacific settlement of international differences."[59] Yet the Contracting Powers were pragmatic enough to foresee their best efforts would not always be sufficient, so they also crafted conventions to "define and govern the usages of war."[60]

An enduring element of these provisions is the desire for humane treatment of all people, even under the most dire of circumstances. Prohibitions on the use of poison, arms that cause superfluous injury, or damage to unprotected individuals or property point to a respect for humanity and recognition that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[61] Similar limitations were also applied to the maritime environments, particularly with regard to protecting commercial traffic and hospital ships.[62] Even the newest weapons of the air were addressed, albeit temporarily.[63] Unfortunately, neither the Hague Conventions, nor the Kellogg-Briand Pact, ratified in 1929, which renounced war as an instrument of national policy, were able to stop the atrocities of World War II. In response to the horrors of concentration camps and the increasing vulnerability of the general population to the ravages of modern industrial war, more comprehensive protections of prisoners and civilians were sought in Geneva.

Geneva Conventions

Though the Hague Conventions and other declarations such as the Paris Declaration on Maritime Law of 1856 and the Lieber Code of 1863 devoted significant consideration to the treatment of neutral parties and prisoners of war, the Geneva

[58] Hague Conference, *Hague I*, 29 July 1899, Articles 20-29 and 18 October 1907, Articles 41-50.
[59] Hague Conference, *Hague I*, Article 1.
[60] Hague Conference, *Hague II*, preamble.
[61] Hague Conference, *Regulations Respecting the Laws and Customs of War on Land*, 29 July 1899, Articles 22 and 23.
[62] Hague Convention III of 1899 and Conventions VI – XIII of 1907.
[63] Hague Convention IV of 1899 prohibited "for a term of five years, the launching of projectiles and explosives from balloons, or by other new methods of similar nature."

Conventions are generally credited with codifying the basic humanitarian rights of individuals in warfare. Starting in 1864 with the *Amelioration of the Condition of the Wounded in Armies in the Field*, which established the Red Cross as an international institution, the conventions continued the attempt to eliminate the most terrible aspects of warfare in 1925 with the *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare*. The treatment of prisoners of war was again addressed in 1929 to reiterate the provisions of the Hague Conventions. These protections were largely successful in World War II, particularly in reference to the use of chemical warfare, but the excesses of bombing campaigns and atrocities in certain prison camps led directly to the Conventions of 1949.

The 1949 Geneva Conventions outline norms of behavior for the treatment of combatants, noncombatants, and property during armed conflict. They include:

- Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field
- Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea
- Convention (III) Relative to the Treatment of Prisoners of War
- Convention (IV) Relative to the Protection of Civilian Persons in Time of War

These restrictions were enhanced in 1977 with the addition of two Protocols relating to the protection of victims of international and non-international armed conflict. The United States has refused to ratify these protocols, claiming they protect terrorist organizations, though the military adheres to most of the articles. The International Red Cross has invoked the principle of *jus cogens* for these protocols, stating that "a number of their articles already form a set of rules of customary law valid for every State, whether or not it is party to the Protocols."[64] The United States *has* ratified the 2005 protocol relating to the adoption of an additional distinctive emblem (red frame diamond) for medical and religious personnel.[65] Ideally all the Geneva Conventions would be

[64] Statement of Cornelio Sommaruga, President of the ICRC, *Appeal by the International Committee of the Red Cross on the 20th anniversary of the adoption of the Additional Protocols of 1977*, 31 October 1997, http://www.icrc.org/web/eng/siteeng0.nsf/html/57JNUX (accessed 23 March 2010).

[65] A full catalog of the Geneva Conventions and Protocols, with listings of state signatories and ratification dates can be found at: http://www.icrc.org/ihl.nsf/CONVPRES?OpenView.

ratified and applied universally, but reality often falls short of the ideal. Nevertheless, they continue to be a shining beacon for the humanitarian conduct of armed conflict.

United Nations Charter

The United Nations was forged on the ashes of the League of Nations after World War II "to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace."[66] Its five principal organs are: the General Assembly, a Security Council, an Economic and Social Council, an International Court of Justice, and a Secretariat (the sixth original body, a Trusteeship Council, was disbanded in 1994 once decolonization was complete.)[67] The United Nations is based on the principle that all Members are sovereign equals and that they "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[68] Thus the Charter effectively banned the legitimate use of force to resolve international disputes and virtually ended the common practice of formally declaring war.

The only exceptions to the use of force are provided in Article 42 by the direction of the Security Council "to maintain or restore international peace and security," and in Article 51 for "the inherent right of individual or collective self-defense." Though this thesis is not necessarily concerned with arguments about *jus ad bellum*, the restriction on use of force is significant because "while international legal norms found in the contemporary U.N. Charter law are helpful, the existing treaty framework is insufficient for solving [the cyberspace] security dilemma since it takes for granted sovereign control and established state responsibility."[69] The next chapter further defines some of the dilemmas inherent in characterizing sovereignty and attribution in cyberspace.

[66] *Charter of the United Nations*, Article 1(1).

[67] *Charter of the United Nations*, Article 7(1).

[68] *Charter of the United Nations*, Article 2(1 and 4).

[69] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law 27*, (2009): 192-251.

Chapter 2

Cyber Law, Doctrine, and Ethics

Where force is necessary, we have a moral and strategic interest in binding ourselves to certain rules of conduct.

-- *United States President Barack Obama*

International actors have attempted to address governance of the Internet since the inception of the World Wide Web. Idealistic libertarians such as John Perry Barlow, John Gilmore, and Mitch Kapor founded the Electronic Frontier Foundation to promote the legal concept of cyberspace as a non-physical territory unto itself.[1] Other Internet founders, led by Vint Cerf, attempted to privatize and internationalize the effort to govern cyberspace with the Internet Society, World Intellectual Property Organization, and the International Ad Hoc Committee.[2] Eventually, non-profit organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) were created to maintain root control over the domain name system and standardize the infrastructure protocols which form the backbone of the Internet. While these institutions have been more or less effective in guiding particular aspects of Internet governance, international arrangements to deal specifically with security and law enforcement are lacking.[3] Despite the efforts of individuals and groups to establish a legal framework for the growth of cyberspace, "international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. U.S. officials must be aware of the implications of their own actions and statements in this formative period."[4] This chapter will investigate the limitations and implications of current cyber law, doctrine, and ethics.

[1] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York, NY: Oxford University Press, 2006), 18.
[2] Goldsmith and Wu, *Who Controls the Internet?*, 37.
[3] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 10.
[4] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, May 1999), 25.

Cyber Law

It is undeniable that "today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain."[5] However, this is not unusual considering that international cyber law has developed "in fits and starts, limited by a lack of universal accord governing these technologies, a disparity in national regulations, and questions of national sovereignty."[6] Also, international cyber law, as such, has only existed for a couple decades—barely enough time to legislate and adjudicate sufficient precedent at the domestic level, to say nothing of the complexities of international implementation. To maintain some semblance of influence and control in cyberspace; however, it is imperative for the United States to be at the forefront of defining and guiding international cyber law.

Some legal scholars suggest that "while an explicit acknowledgement of the problem through the United Nations would be an ideal solution, it is more likely that smaller bilateral and multilateral agreements between states will break the trail in rulemaking in the Internet realm."[7] The primary reason for this is that "deeply held differences in values, even among democracies, lie behind conflicts of laws," and it is very difficult to reach a consensus on the proper way to control Internet activity at an international level.[8] However, governments, businesses, and individuals alike realize the importance of a certain level of reliability and cooperation in the global system. In a Green Paper published in 1998, the United States declared four shared principles for the Internet: stability; competition; private, bottom-up coordination; and representation.[9]

Multinational corporations quickly discovered that in order to conduct business online they "would depend critically on government coercion and the rule of law provided by a stable country like the United States. These are a few of the many complex

[5] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, eds. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Committee on Offensive Information Warfare, (Washington, DC: The National Academies Press, 2009), 4.

[6] Jon P. Jurich, "Cyberwar and Customary International Law," *Chicago Journal of International Law 9*, no. 1 (Summer 2008): 275-294.

[7] Wolfgang McGavran, "Intended Consequences: Regulating Cyber Attacks," *Tulane Journal of Technology and Intellectual Property 12*, (Fall 2009): 259-275.

[8] Goldsmith and Wu, *Who Controls the Internet?*, 152.

[9] United States Department of Commerce, *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule*, US Government Green Paper, National Telecommunications and Information Administration, (Washington, DC: Federal Register, 20 February 1998), 15 CFR Chap. XXIIII, Vol. 63, No. 34, pg. 8827, http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.txt.

benefits that only territorial sovereigns can bring, and without which most aspects of the Internet that we love and cherish would not exist."[10] This is primarily because national governments are the primary enforcers of contracts and laws governing the telecommunications infrastructure upon which the Internet and those who interact online depend. It is conceivable that an international authority might be able to enforce law and assure stability and representation in the future; yet, despite repeated efforts to establish such an institution, the power of legitimate law enforcement has remained within nation-states.

Business is not the only context where cyberspace norms are coalescing: "While controlling [the Internet] is primarily about money in some countries, in other countries it plays a pivotal role in freedom of speech."[11] The power of a national government to restrict or allow freedom of expression online is one of the most significant issues of contention in contemporary international politics. Google is one of many institutions that have been involved in litigation over privacy and security infringements in China, Italy, and the United States to name just a few cases.[12] The company eventually decided to withdraw its search engine capability and reroute server requests to locations outside China over accusations of cyberattacks and censorship.[13] This incident resulted in a major policy statement by the United States Secretary of State, which introduced the notion of a new universal right—the freedom to connect.[14]

While these disputes may not be directly applicable to cyberwarfare, they set a "chilling precedent ... to expect firms to monitor everything that goes online" and provide protection for "critical components on which our economy, government and national

[10] Goldsmith and Wu, *Who Controls the Internet?*, 129.

[11] Scott P. Sonbuchner, "Master Your Domain: Should the U.S. Government Maintain Control over the Internet's Root?" *Minnesota Journal of International Law 17*, (Winter 2008): 183-207.

[12] Chris Matyszczyk, "Google Gets Buzzed With Class Action Lawsuit," *CNET News*, 17 February 2010, http://news.cnet.com/8301-17852_3-10455573-71.html (accessed 24 February 2010); Jim Wolf, "Google Puts Focus on China Cyberwar Fears," *Reuters*, 20 January 2010, http://www.reuters.com/article/idUSTRE60J5PK20100120 (accessed 21 January 2010); Jane Wakefield, "Google Bosses Convicted in Italy," *BBC News*, 24 February 2010, http://news.bbc.co.uk/2/hi/technology/8533695.stm (accessed 24 February 2010).

[13] This has been a fascinating debate in the international community over nearly all aspects of cyberspace norms from freedom of access and connectivity, to freedom from control, monitoring, and censorship. Numerous articles have been published since the incident started in January 2010, one describing the culmination is: Deborah Tedford, "Google to Shift Chinese Users to Hong Kong," *NPR*, 22 March 2010, http://www.npr.org/templates/story/story.php?storyId=125028043&sc=emaf (accessed 22 March 2010).

[14] Hillary Rodham Clinton, "Remarks on Internet Freedom," (speech, Newseum, Washington, DC, 21 January 2010) http://www.state.gov/secretary/rm/2010/01/135519.htm.

security are based" while simultaneously holding them accountable for "compromising the confidentiality of a computer."[15] These incredibly complex situations blur the lines of distinction between government and corporate policy. They also call into question the amount of control a nation-state has, or should have, over the actions of its citizens, and the extent of a state's sovereignty in cyberspace. A bevy of domestic and international law has been enacted over the past quarter century to manage conflicting requirements for access, privacy, security, and control. As with all bodies of knowledge, the law is continually interpreted and amended to reflect experience, and cyberspace is the epitome of an environment in flux—the law has barely kept pace.

Domestic Law

Some scholars believe federal legislation is not sufficient to deter cyberwarfare, and that "Congress should enact new, comprehensive anti-hacking legislation that would give federal prosecutors further investigative authority and prosecutorial power to counteract foreign-government-sponsored hacking."[16] Domestic law will hardly be sufficient to secure an environment that is open, anonymous and internationally interconnected. Domestic law strongly influences international law, however, and numerous laws have been used to increase cyber security and prosecute those responsible for computer attacks globally. A partial list of applicable United States' laws and a brief description of each can be found in Appendix A.[17]

Domestic law to date has been primarily concerned with prosecuting fraud and abuse, protecting privacy and financial information, ensuring the security of trade secrets and government systems, and in some countries directing the content provided. In the future, it may be necessary to pass laws requiring internet service providers to register users, set minimum security conditions on critical infrastructure, or increase the level of monitoring and control on certain sectors of cyberspace. These ideas are further investigated in Chapter four and the Conclusion. However, a comprehensive solution will only be realized through international cooperation.

[15] Matyszczyk, "Google Gets Buzzed With Class Action Lawsuit."; Wolf, "Google Puts Focus on China Cyberwar Fears."; Wakefield, "Google Bosses Convicted in Italy."

[16] Jonathan Eric Lewis, "The Economic Espionage Act and the Threat of Chinese Espionage in the United States," *Chicago-Kent Journal of Intellectual Property* 8, no. 2 (Spring 2009): 189-236.

[17] Another list was compiled in John Moteff, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, Congressional Research Service Report (Washington, DC: Library of Congress, 16 April 2004).

International Law

Despite the fact that "reliance on decentralized economic and legal decision-making has become a common feature of Internet behavior," the underlying stability of the Internet still relies on the rule of law within nation-states; however, it will increasingly depend on international cooperation.[18] Although some say "in many of the key forums, particularly those related to the standards process that is fundamental to the Internet, private parties dominate and governments play only a subordinate role," nation-states are still able to control the direction of events through traditional methods of government coercion.[19] For instance, regulations on Internet service providers, edicts concerning censorship and privacy, and punishments for computer hacking all depend on domestic law enforcement. While it is true that these restrictions may not apply during a conflict, "the international legal framework to deal with cyber attacks is severely underdeveloped."[20] In fact, say military lawyers, "International communications law contains no direct or specific prohibition against the conduct of [computer network attack] or other information operations by military forces during armed conflict or in response to aggression."[21]

This freedom of action could be an advantage on the offensive, because without conventions against cyberattack an aggressor cannot be condemned in the international courts of justice or public opinion. However, on the defensive, it becomes a liability, because, "the lack of any international agreement explicitly addressing computer attacks between nations creates an equally ambiguous legal course of action for any victim nation."[22] The situation is convoluted further by lack of attribution, since "the supposed target can claim an attack that may not have happened from someone who probably did

[18] Marcelo Halpern and Ajay K. Mehrota, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age," *University of Pennsylvania Journal of International Economic Law 21*, (Fall 2007): 523-561.

[19] Harold Kwalwasser, "Internet Governance," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 491.

[20] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law 27*, (2009): 192-251.

[21] James P. Terry, "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Conflict: What are the Targeting Constraints?" *Military Law Review 169*, (September 2001): 70-89.

[22] Daniel M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China," *American University International Law Review 17*, (2002): 641-681.

not do it [thus] supporting norms that legitimize cyberdeterrence may give less fastidious governments yet one more excuse to wreak international mischief."[23] An international quorum denouncing all forms of cyberattack may reduce the ambiguity, but "until a new legal regime can be erected to deal with the threat of cyber warfare and cyber terrorism, actors in this emergent field will be forced to fit these new forces by analogy into the currently unwieldy international law of war."[24]

Some consensus on international cyber law will be necessary to regulate the Internet on a global scale. This is important not only for cybercrime and cyberterrorism, but it could aid in identifying the limits of cyberwar. "Today, governance of the cyber commons is a messy amalgamation of international, national, and non-state protocols and agreements—all of which are sufficient for cyberspace to flourish but insufficient to make it safe."[25] While the current law of armed conflict (LOAC) can be applied to cyberspace, there are idiosyncrasies, such as the definition of sovereignty and the impact of communications protocol standards on the environment that will require unique solutions. A few existing international and multilateral agreements can act as models for a future system of cyberspace governance.

International Telecommunications Union

The ITU started in 1865 as the International Telegraph Union, so obviously it was not specifically designed to control cyberspace, though one could argue that the telegraph was cyberspace in the nineteenth century. Regardless, it is now a sub-agency of the United Nations, with 191 national governments represented as voting members and over 700 sector members and associates, who "for nearly 145 years, [have] coordinated the shared global use of the radio spectrum, promoted international cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards that foster seamless interconnection of a vast range of communications systems and addressed the global challenges of our times, such

[23] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND corporation, 2009), 51-52.
[24] McGavran, "Intended Consequences: Regulating Cyber Attacks," 259-275.
[25] Abraham M. Denmark et al. eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security Report, January 2010, (accessed 12 February 2010), 150 http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.

as mitigating climate change and strengthening cybersecurity."[26] A long and successful history is one reason why "there are considerable pressures to diminish U.S. influence by increasing the ITU's role in Internet governance."[27] Some have suggested that a new agency be created based on the ITU, but "designed to reflect the particular needs and nature of the largely self-regulated cyber world."[28] Others feel this type of international institution could be manipulated "to allow authoritarian states like China to use it to repress their populations or restrict the free flow of ideas."[29] A well-respected international organization like the ITU might help with the administration of Internet standards, which are currently handled by ad hoc non-governmental organizations such as ICANN and IETF, but enforcement authority will still be required to address actors who violate the law and transgress norms of behavior in cyberspace.

Council of Europe Convention on Cybercrime

One of the first multilateral agreements to address the growing problem of cyberattacks was the Convention on Cybercrime, signed in 2001 and ratified by the United States in 2006.[30] This loosely defined treaty recognizes that an "effective fight against cybercrime requires increased, rapid and well-functioning international co-operation."[31] Offenses include such acts as illegal access, illegal interception, data or system interference, misuse of devices, forgery, fraud, child pornography, copyright infringement, or aiding and abetting in any infraction.[32] The signatories are expected to adopt national safeguards, sanctions, and liability laws to expedite investigation and

[26] International Telecommunications Union, "About ITU," http://www.itu.int/net/about/index.aspx (accessed 20 February 2010).

[27] Kwalwasser, "Internet Governance," 513.

[28] The Agency for Information Infrastructure Protection was proposed by Abraham D. Sofaer and Seymour E. Goodman, *A Proposal for an International Convention on Cyber Crime and Terrorism* (Stanford, CA: The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP), and The Center for International Security and Cooperation (CISAC), August 2000), (accessed 1 April 2010) http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf.

[29] House, *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Testimony before the Committee on Foreign Affairs*, 10 March 2010, 8.

[30] A very similar convention was offered but not adopted around the same time period by Sofaer and Goodman, *Proposal for an International Convention on Cyber Crime and Terrorism*.

[31] Council of Europe, *Convention on Cybercrime* (Budapest, Hungary: European Treaty Series No. 185, 23 November 2001), Preamble.

[32] Council of Europe, *Convention on Cybercrime*, Articles 2-11.

prosecution of criminals across sovereign borders, including the real-time collection and preservation of data and mutual assistance for extradition.[33]

Even in this minimal and preliminary attempt at governance, critical deficiencies in forming collective norms of behavior are evident "in view of the fact that over 150 States within the international community are not party to the Convention. The difficulties of creating appropriate global legal norms for cybercrime are further increased since the claim that the Convention is codifying common legal norms of international law is difficult to justify."[34] Deeply-held cultural differences on what constitutes a moral and ethical infraction lead to diplomatic impasses. For instance, the United States refused to ratify the treaty protocol criminalizing racist language on the Internet due to Constitutional guarantees for freedom of expression. Notable non-signatories are China and Russia, who object to the treaty based on supposed infringement of state sovereignty. The fracas concerning censorship between Google and China shows how disagreements about privacy, access, monitoring, and basic freedoms can impede collaboration.[35] Thus, even in the cybercrime context where there is a general consensus about the need for cooperation, it is very hard for nations to agree due to concerns over sovereignty and societal control.

Cyber Doctrine

Former Air Force Deputy Judge Advocate General, Major General Charles Dunlap Jr., highlights the importance of a full-spectrum response to cyber security: "[Simply] because a particular cyber-related matter has a national security dimension does not mean, necessarily, that it is appropriate for the armed forces to address."[36] Indeed by its very nature, cyberspace requires an interagency and international approach. The latest Quadrennial Defense Review demands that the Department of Defense "needs to collaborate with other U.S. departments and agencies and international partners, both

[33] Council of Europe, *Convention on Cybercrime*.
[34] Andreas Fischer-Lescano & Gunther Teubner, "Reply to Andreas L. Paulus Consensus as Fiction of Global Law," *Michigan Journal of International Law 25*, (Summer 2004): 1059-1073. A listing and visual presentation of the signatories of the Convention can be found in Appendix C.
[35] Jim Wolf, "Google puts focus on China cyberwar fears," *Reuters*, 21 January 2010, http://www.reuters.com/article/idUSTRE60I4PA20100121 (accessed 21 January 2010).
[36] Major General Charles J. Dunlap, Jr., "Towards a Cyberspace Legal Regime in the Twenty-First Century," (speech, Air University 2008 Cyberspace Symposium, Maxwell AFB, AL, 16 July 2008).

to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense."[37] The defense of cyberspace may eventually require greater cooperation from nongovernmental agencies and international partners, but the United States government has only just begun to lay the foundation for a solid cyberspace doctrine at the national, agency, and service levels.

Executive Directives

There are a host of executive directives guiding telecommunications and cyber security. Some of the first that are still operative are Executive Orders 12382 (President's National Security Telecommunications Advisory Committee) and 12472 (Assignment of National Security and Emergency Preparedness Telecommunications Functions), signed by President Ronald Reagan in 1982 and 1984 respectively, to ensure the nation's communications systems are survivable and responsive to the national command authority. National Security Directive 42, signed July 5, 1990 by President George H. W. Bush, established the National Security Telecommunications and Information Systems Security Committee, now known as the Committee on National Security Systems, which "provides a forum for the discussion of policy issues, and is responsible for setting national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government."[38] The Clinton administration's Presidential Decision Directive 63, Critical Infrastructure Protection, made cyberattack against key United States assets equivalent to a physical attack.

President George W. Bush established a National Infrastructure Advisory Council on 16 October 2001, and signed Executive Orders 13231 (Critical Infrastructure Protection in the Information Age), and 13286 (Transfer of Certain Functions to the Secretary of Homeland Security) in 2001 to solidify and consolidate the nation's defense

[37] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 39.

[38] The Committee on National Security Systems, "CNSS History," http://www.cnss.gov/history.html (accessed 24 March 2010).

of cyberspace.[39] The second Bush administration also developed a National Strategy to Secure Cyberspace in 2003, with three strategic priorities:

- Prevent cyber attacks against America's critical infrastructure
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks

Finally, after the Estonia and Georgia cyberattacks and increasing intrusions on United States systems, the administration launched the Comprehensive National Cyber Security Initiative in January 2008 to protect federal government systems from cyber espionage with classified Homeland Security Presidential Directive 23/National Security Presidential Directive 54. There have been numerous other classified directives concerning cyberspace, which are unfortunately outside the scope of this document. The Obama administration has continued the focus on cyber security with a Cyberspace Policy Review, and is working with the Department of Defense and National Security Agency to establish a United States Cyber Command.[40]

Department of Defense

Despite the Department of Defense's intimate involvement with the development of cyberspace, or perhaps because of it, United States military cyber doctrine has been shrouded in secrecy. Doctrine written specifically for cyberspace is still in draft, because the Department of Defense and national command authorities have not, until recently, decided how they would address command and control of this domain. While considerable effort has been expended building the capabilities of Department of Defense networks, an articulate doctrine for securing the environment beyond individual training and awareness continues to elude the military.

There are four strategic priorities in the 2006 *National Military Strategy for Cyberspace Operations*:

- Gain and maintain initiative to operate within adversary decision cycles
- Integrate cyberspace capabilities across the range of military operations
- Build capacity for cyberspace operations
- Manage risk for operations in cyberspace

[39] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Government Printing Office, 2009), 145-146.

[40] United States Cyber Command stood up on 21 May 2010.

Joint Publication 3-13, Information Operations includes two core capabilities that can be considered explicitly cyber: electronic warfare and computer network operations, though the others—psychological operations, military deception, and operations security—also play a major part of military operations online. This document highlights the criticality of timely and accurate intelligence when conducting cyber operations. It also recognizes various legal restrictions imposed on the environment, and the importance of integrating planning and execution of information operations with other forms of warfare.

The stated purpose of information operations is "to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[41] The information environment is divided into three dimensions—physical, informational, and cognitive—and influencing the latter is the most important to achieving results.[42] This doctrine also cogently points out that "targeting automated decision making, at any level, is only as effective as the human adversary's reliance on such decisions."[43] Thus a prudent precaution for defensive purposes would be to ensure that our own processes are not overly reliant on any automatic system.

Computer network operations are divided into computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE). CNA consists of actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity from both internal and external adversaries on DOD information systems. CNE enables operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[44] Doctrinal employment of these capabilities is published in a classified appendix. While it is important to keep specific methods hidden from potential enemies, the secrecy that shrouds much of cyber doctrine impairs effective integration of these tools into normal operations and contributes to a misunderstanding of the possibilities and limitations of this valuable instrument of national power.

[41] Joint Publication 3-13, *Information Operations*, 13 February 2006, I-1.
[42] Joint Publication 3-13, *Information Operations*, 13 February 2006, I-2.
[43] Joint Publication 3-13, *Information Operations*, 13 February 2006, I-9.
[44] Joint Publication 3-13, *Information Operations*, 13 February 2006, II-5.

Air Force Doctrine

The Air Force attempted to seize the initiative in cyberspace with the introduction of Air Force Cyber Command in 2007, but this venture was thwarted by interservice rivalry and intraservice turmoil and ended on 6 October 2008.[45] Instead the Air Force stood up an apparently less threatening numbered air force in August 2009 to consolidate existing cyberspace activities. The 24th Air Force is still in its infancy and the draft version of Air Force Doctrine Document 3-12, *Cyberspace Operations* looks remarkably similar to the older and also draft version of Air Force Doctrine Document 2-11, *Cyberspace Operations*, but progress is being made. Officials have noted, however, that "we will never be able to operationalize cyberspace to the same extent as has been done with the air weapon, absent a renewed effort to reduce the classification levels."[46]

Some of the foundational doctrine statements of AFDD 2-11 are:

- Ensuring freedom of action in cyberspace is a complex undertaking that requires comprehensive situational awareness, understanding of relevant network segments, and an exceptionally fast decision cycle.
- Cyberspace superiority is the degree of dominance in cyberspace of one force over another that permits the conduct of operations by the former and its related land, air, sea, space, and special operation forces at a given time and place without prohibitive interference by the opposing force
- Defensive operations seek to deter adversaries from intruding on friendly networks, detect and deny access when attacks are attempted, minimize the effectiveness of attacks, and determine their source(s).
- Offensive operations deny, degrade, disrupt, destroy, alter, or otherwise adversely affect an adversary's ability to use cyberspace.
- US forces should be capable of operating through a cyberspace attack. They should recognize and isolate an attack while continuing to perform critical actions. Following an attack, they should be able to reconstitute and regenerate capability rapidly.

[45] Noah Shacthman, "Air Force Suspends Controversial Cyber Command," *Danger Room, Wired.com*, 13 August 2008, http://www.wired.com/dangerroom/2008/08/air-force-suspe/ (accessed 29 March 2010).
[46] Maj Gen Charles J. Dunlap, Jr., "Towards a Cyberspace Legal Regime in the Twenty-First Century," (speech, Air University 2008 Cyberspace Symposium, Maxwell AFB, AL, 16 July 2008).

One very poignant paragraph in AFDD 3-12 notes, “The nature of cyberspace, government policies, and international laws and treaties makes it very difficult to determine the origin of a cyberspace attack. The ability to hide the source of an attack makes it difficult to connect an attack with an attacker within the cyberspace domain. The design of the Internet lends itself to anonymity.”[47] This vulnerability underlines the need to modify the current architecture, policy, or norms of behavior in cyberspace to neutralize the impact of anonymity. However, this transformation must be promulgated globally, because “some cyberspace users have similar ways and intents of using cyberspace to our own. Other users (possible adversaries) often operate in ways not constrained by our laws or moral values.”[48] Allied operations are evaluated within a legal framework established by, “international law, domestic law and policy decisions, the law of armed conflict, and rules of engagement,” but other actors may not be subjected to the same restrictions.[49] The only way to encourage this type of systemic change is through the application of soft power to alter the underlying ethics of cyberspace conduct.

Cyber Ethics

The growth of the Internet can only be described as viral. Though it started with a small group of idealistic engineers with virtuous intentions; cyberspace has quickly evolved to encompass the full range of human thought and emotion—good and bad. Certain aspects of Internet architecture and usage have generated a unique set of ethics for cyberspace. For instance, “The scourge of spam, which clogs the Internet with some 15 billion e-mail messages a day, is provoking powerful responses. It's pushing companies and individuals alike to install new tools and adopt norms for online behavior.”[50] These norms of behavior reflect disparate expectations of cyberspace concerning: access and connectivity; trust and security; privacy and anonymity; and monitoring and control.

[47] Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 9.
[48] Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 15.
[49] Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 30.
[50] Stephen Baker, “Taming of the Internet,” *Business Week*, 15 December 2003, http://www.businessweek.com/magazine/content/03_50/b3862091_mz063.htm.

In fact, norms of behavior both influence, and are influenced by, our expectations of the online experience—expectations which are dependent on "different backgrounds, capacities, preferences, desires, and needs [which] reflect local differences in history, culture, geography, and wealth."[51] The disparity in developing international norms of behavior has therefore generally been caused by the informal approaches of various nation-states.[52] According to Kurt Wimmer, an international lawyer based in Washington DC, this has caused major problems, because "countries currently have no realistic process for even beginning to discuss how to achieve an accommodation between one country's ability to support the free speech of its citizens and another country's desire to restrict the availability of certain content."[53] For instance, the expectation for freedom of expression in the United States was challenged by a French court in the case of *Association Union des Etudiants Juifs de France v. Yahoo! Inc.* when La Ligue Contre Le Racisme et L'Antisemitisme sued to have Nazi paraphernalia removed from an auction site on a server in the United States, but accessible to users in France. Likewise, in *Dow Jones & Co. v. Gutnick*, an Australian court found that *Barron's* magazine could be held liable for libel under Australian law despite the fact that it was published in New Jersey and 99 percent of its subscriptions were in the United States.[54] Both of these cases and others like them have been adjudicated against the American companies in favor of the domestic laws of the country in which the suit was filed. As Wimmer protests, "These cases are characterized less by thoughtful analysis of international norms than simple nationalistic determinations that 'publication' occurs wherever the citizens of any state in the world can be injured by speech published on the Internet.[55]

These disputes may seem trivial when contrasted with the moral dilemmas extant in armed conflict, but norms created in peace shape the basic expectations of moral and ethical behavior in war. Also, human rights violations of dignity and equality, and limitations on freedom of expression and access to information often leads to open

[51] Goldsmith and Wu, *Who Controls the Internet?*, 149.
[52] Jurich, "Cyberwar and Customary International Law," 275-294.
[53] Kurt Wimmer, "International Processes: Toward a World Rule of Law: Freedom of Expression," *The Annals of The American Academy of Political and Social Science 603*, (January 2006): 202-216.
[54] Wimmer, "International Processes," 202-216.
[55] Wimmer, "International Processes," 202-216

violence. The United States in particular "has been steadfast in supporting liberty, freedom, and open access to markets and ideas."[56] The following sections examine the principal norms of behavior that are forming in cyberspace.

Access and Connectivity

Social networking and search engines secured cyberspace's role as a domain for global influence. Governments, industries, and individuals have come to rely on instantaneous access and connectivity through cyberspace to the world market for business, pleasure, and maintenance of everyday life. By some accounts, "dependable access to the commons is the backbone of the international economy and political order."[57] Ubiquity of wireless, broadband, personalized information has engendered a new universal right—freedom to connect. As Secretary of State Hillary Clinton summarized in a recent speech, "Countries that restrict free access to information or violate the basic rights of internet users risk walling themselves off from the progress of the next century.... Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society."[58]

However, according to Jack Goldsmith and Tim Wu, "information does not, in fact, want to be free. It wants to be labeled, organized, and filtered so it can be discovered, cross-referenced, and consumed."[59] All of the information in the world is useless unless it is accessible and searchable within a reasonable amount of time. The norms of access and connectivity have resulted in an expectation for near instant availability to any requested information in a readily coherent format, and an increasing reliance on immediate, direct telecommunication.

This is not a universal expectation, of course, as many countries censor information before it becomes accessible. Wimmer points out that "countries' unrestrained application of their own, often more restrictive, laws against Internet content could [deny] large portions of the world's population the ability to receive diverse sources

[56] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 9.
[57] Abraham M. Denmark et al. eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security Report, January 2010, (accessed 12 February 2010), 5 http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.
[58] Clinton, "Remarks on Internet Freedom."
[59] Goldsmith and Wu, *Who Controls the Internet?*, 51.

of information."[60] This could lead to a balkanization of the Internet, and a "legal hell: a world of Singaporean free speech, American tort law, Russian commercial regulation, and Chinese civil rights."[61] It would also mean a significant decline in access and connectivity to alternative points of view, and a regrettable hindrance to peace and understanding in the global community. Wimmer concludes that if access is limited by censorship or isolation in the name of security, "the essential character of the Internet will be altered and its capacity to act as a universal source of information will be lost."[62]

Despite intermittent bouts of isolationism, the United States has always been a champion of unimpeded access to economic markets, open diplomatic connectivity, and freedom of information. The norms of open access and connectivity in cyberspace enhance the pursuit of universal democratic principles and a liberal economic world order. Thus they are in the best interest of the United States and other like-minded nations. Unfortunately, as Pericles admits in his famous funeral oration, "the eyes of an enemy may occasionally profit by our liberality," so we must rely on other norms of cyberspace behavior to protect our interests.[63]

Trust and Security

Franklin Kramer states baldly, "The cyberworld is not secure. Each level of cyber—physical infrastructure, operational software, information, and people—is susceptible to security breakdowns whether through attack, infiltration, or accident."[64] Cyberspace users rely on cryptology, operational procedures, and physical security measures to provide the trust and security necessary to function effectively online. Companies understand that "it no longer matters if an online offering is cool, fun, useful, and easy-to-use if it's not secure."[65] Trust and security have become cyberspace norms that provide a foundation for the Internet economy, global diplomacy, and a networked military, but it is a foundation in perpetual danger of collapse.

The original Internet architecture was "configured in a manner reflecting the fact that the network was unreliable and the trust anchors were ... known to each other.

[60] Wimmer, "International Processes," 202-216.
[61] Goldsmith and Wu, *Who Controls the Internet?*, 7.
[62] Wimmer, "International Processes," 202-216.
[63] Robert B. Strassler, *The Landmark Thucydides* (New York, NY: Simon & Schuster, 1996), 2.39.
[64] Kramer, "Cyberpower and National Security," 6.
[65] Stephen Baker, "Taming of the Internet," *Business Week*, 15 December 2003, (accessed 16 February 2010) http://www.businessweek.com/magazine/content/03_50/b3862091_mz063.htm.

Today, the opposite holds true: the networks are trustworthy and work, but the people are not well known and cannot be relied upon."[66] This has only exacerbated the traditional mistrust many people have of solicitors and intrusive government agencies. The ability to attain and maintain massive databases has not only driven profitable legal adware and illegal spyware industries, but enabled both the growth of trust networks for banking and business as well as the capacity to falsify these networks for nefarious purposes. As one journalist puts it, the result seems like "betrayal. That's what pioneering computer scientists feel when they see what has happened to the Internet. They built a miraculous system with a foundation of trust, and it's being overrun by scoundrels."[67] This trust was well-founded when the network was populated by a handful of academics looking to share research, but now that it is being used to share everything from porn to state secrets the trust is no longer warranted.

With the advent of botnets and viral worms, there is no longer even a guarantee that the system in question is being operated directly by a human. Though the most insidious and effective assaults are certainly controlled by highly skilled individuals, the most common form of attack—a distributed denial of service—enlists the unwitting support of tens of thousands of zombie computers. The botnet builders and other hackers engage in a constant battle with intrusion detection experts and network administrators. Captchas, digital encryption keys, and firewalls are just a few of the myriad methods used to ensure there is a person on the other end of a transaction, and that they are indeed who they say they are.[68] Other authors have suggested the need for a change in the standard transmission format from a packet-based to session-based protocol which requires "positive identification of end-point users before access is granted."[69] A thriving industry has grown around providing measures of trust and security in cyberspace. There are many technological methods for ensuring increased security, from daily updated virus signature libraries to anomaly detection algorithms, but one of the most effective

[66] Paul Rosenzweig, "National Security Threats in Cyberspace" (workshop report, American Bar Association Standing Committee on Law and National Security, Annapolis, MD, 4-5 June 2009), 22.

[67] Baker, "Taming of the Internet."

[68] The most comprehensive compilation of information security principles and practices can be found in: Information Security Forum, *The Standard of Good Practice for Information Security*, 2007, https://www.isfsecuritystandard.com/SOGP07/pdfs/SOGP_2007.pdf (accessed 25 March 2010).

[69] John C. Rogers, *Shaping the Air Force Operational Environment in Cyberspace* (Air War College research report, Maxwell AFB, AL: Air University, 12 February 2009), 24.

techniques is air-gapping certain critical and sensitive systems—disconnecting them from the publicly accessible Internet.

For example, the United States government has created a series of classified networks including the Secret Internet Protocol Router Network (SIPRNet) and the Joint Worldwide Intelligence Communications System (JWICS). The financial industry has a similar system in the Society for Worldwide Interbank Financial Telecommunication Network (SWIFTNet) used for secure transactions. While these isolated networks are effective for specialized operations, isolating them from the rest of cyberspace can limit their usefulness, and they can still be vulnerable if strict physical and operational security is not maintained. Military networks also use some of the same servers, satellites, and cables as unsecure civilian networks, which can complicate the separation of combatants and noncombatants. This not only accentuates the importance of individuals, physical assets, and procedural controls to the security of the system, it points to the next norms of behavior in cyberspace, and a major weakness in the foundation of trust and security.

Privacy and Anonymity

Legal scholars submit that "the online right to privacy developed organically into what is now a cherished cyberspace custom."[70] Privacy is a deeply-rooted principle of Western culture, but it is far from being an international standard, despite its institution in Article 12 of the Universal Declaration of Human Rights.[71] Likewise anonymity has long been central to freedom of expression, used by political activists such as the authors of the Federalist Papers to publicly communicate dissenting opinions without fear of oppression or reprisal. Conflating privacy with anonymity, however, can be problematic because it confuses the issue of human rights violations with the security issue of attribution. While protection of privacy is a worthy cause, protection of unfettered anonymity can invite abuse by those who intend harm.

The QDR sheds light on the threat: "The speed of cyber attacks and the anonymity of cyberspace greatly favor the offense. This advantage is growing as hacker

[70] Marcelo Halpern and Ajay K. Mehrota, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age," *University of Pennsylvania Journal of International Economic Law 21,* (Fall 2007): 523-561.

[71] United Nations General Assembly, *The Universal Declaration of Human Rights*, 10 December 1948, Article 12. Found at: http://www.un.org/en/documents/udhr/index.shtml states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication."[72] In fact by some estimates, "only 5 percent of cyber criminals are ever arrested or convicted, because the anonymity associated with Web activity makes them hard to catch and the trail of evidence needed to link them to a cyber crime is hard to follow."[73] Experts now say that the cyberspace environment has degraded to the point that "new systems must now be engineered with the assumption that everyone is a possible hacker or thief."[74] Disassociating the right to privacy from the cyberspace norm of anonymity is in the best interest of nation-states that want to curb cybercrime and increase the strength of cyber deterrence, because attribution is critical to these pursuits.

This position is not without detractors, as many who distrust government access to personal information would rather stay anonymous. The Electronic Frontier Foundation, Global Network Initiative, and Privacy International are three prominent defenders of online anonymity, privacy, and freedom of expression.[75] Other organizations such as Wikileaks flaunt their ability to find and reveal government secrets.[76] The Global Internet Freedom Consortium has been working for several years to break through China and Iran's firewalls to maintain the anonymity of millions of Internet users.[77] Secretary of State Clinton expresses the dilemma of anonymity: "On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments."[78] Finding the balance between freedom of expression and protection from exploitation is one of the basic conundrums of governance.

[72] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 37.

[73] Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 428.

[74] Baker, "Taming of the Internet."

[75] These organizations can be found at: http://www.eff.org/, http://www.privacyinternational.org/, and http://www.globalnetworkinitiative.org/.

[76] Wikileaks "accepts classified, censored, or otherwise restricted material of political, diplomatic, or ethical significance" and has been called an "uncensorable and untraceable depository for the truth." https://secure.wikileaks.org/

[77] Ethan Gutmann, "Hacker Nation: China's Cyber Assault," *World Affairs Journal*, May/June 2010, http://www.worldaffairsjournal.org/articles/2010-MayJune/full-Gutmann-MJ-2010.html. Global Internet Freedom Consortium can be found at: http://www.internetfreedom.org/.

[78] Hillary Rodham Clinton, "Remarks on Internet Freedom," (speech, Newseum, Washington, DC, 21 January 2010). http://www.state.gov/secretary/rm/2010/01/135519.htm.

One way of dealing with the issue of anonymity has been to strengthen controls. For instance, China has been creating alternatives to foreign computer technologies and websites like YouTube, Facebook and Twitter, all of which are monitored by censors. The government claims it needs these controls to fight pornography, piracy, and other illegal activity, but they have been known to screen search engines, blogs, and emails for "politically sensitive terms, such as 4 June (the date of the Tiananmen Square crackdown), human rights, independent Taiwan or Tibet, and Falun Gong."[79] The draft version of Air Force Doctrine Document 3-12, *Cyberspace Operations*, points to this same solution: "nations have the advantage of law and the ability to modify the technological environment by fiat."[80] In other words, changing the architecture of cyberspace could allow greater or lesser transparency, and properly worded laws could ensure or restrict privacy while eliminating the sanctuary of anonymity. While this may overstate the power of individual nation-states to effect change over the entirety of cyberspace, the previous section points to some specific measures that could be taken to limit anonymity and increase the trust and security of computer networks.

When criminals mix legal and illegal activity, it gives a free government "no choice but to lose what it likes when it bans what it doesn't like. It means taking advantage of deeply held national values, like commitments to open commerce, free speech, or respect for citizen privacy."[81] These principles, inherent to Western-style democracies, have certainly been taken advantage of to promote messages of hate and to hide activities antithetical to freedom, but this is part of the eternal balancing act between privacy and security. Despite the apparent chaos, nation-states, multinational corporations, and individuals can actually exert considerable authority over specific sections of cyberspace with intrusion detection and prevention systems and other positive identification techniques used for monitoring and control.

Monitoring and Control

Internet users regularly submit to monitoring and control in return for access privileges to particularly useful applications, such as Paypal, eBay, and most banking and

[79] Tim Luard, "Chinese Activists Evade Web Controls," *BBC online*, 30 January 2004, http://news.bbc.co.uk/2/hi/asia-pacific/3440911.stm (accessed 17 May 2010).
[80] Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 9.
[81] Goldsmith and Wu, *Who Controls the Internet?*, 83.

federal government sites. Some technology actually increases the potential for monitoring and control. "The increased use of Wi-Fi, for example, will make it easier to track people geographically through radio signals and satellites. And rising Net activity on portable devices like web-enabled phones will permit easier geographical tracking through Global Positioning Systems that are built into the phones."[82] While criminals and other unsavory characters will continue to more or less successfully avoid them, monitoring and control measures have undoubtedly become an accepted norm of cyberspace.

Some nation-states are more inclined to enact stricter restraints on cyber behavior. For instance, "Chinese leaders are constantly trying to balance the economic and social benefits of online freedoms and open communications against the desire to preserve social stability and prevent organized political opposition."[83] One way to do this is through constant monitoring: "Today, regulations in cities like Shanghai ... require users to register with their national ID card before logging on."[84] Another method is to nationalize services such as search and email, like Russia, Iran, and Turkey have done.[85] The trends toward tighter monitoring and control can clearly be seen: "Where traditional Internet communications are unfettered, open, and chaotic, look for the next generation to be far more regulated, orderly, and closed."[86]

Limitations already exist to a great degree on financial and military networks, and will be more common on public networks as private corporations and governments install tighter security measures. In testimony to the House of Representatives Committee on Foreign Affairs, a commissioner on the U.S.-China Economic and Security Review Commission, Larry Wortzel, suggested that increased malicious activity from Chinese and Russian sources requires that "scanning should be expanded to include monitoring activity on critical infrastructure networks and on defense contractors."[87] These

[82] Goldsmith and Wu, *Who Controls the Internet?*, 62.

[83] Sharon LaFraniere and Jonathon Ansfield, "China Alarmed by Security Threat from the Internet," *New York Times*, 11 February 2010, http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html (accessed 16 February 2010).

[84] Goldsmith and Wu, *Who Controls the Internet?*, 97.

[85] Evgeny Morozov, "Is Russia Google's Next Weak Spot?" *Foreign Policy: Net Effect*, 26 March 2010, http://neteffect.foreignpolicy.com/blog/5386 (accessed 30 March 2010).

[86] Baker, "Taming of the Internet."

[87] House, *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Testimony before the Committee on Foreign Affairs*, 10 March 2010, 7.

precautions are also necessary due to non-state threats, since “Jihadists are not an idle enemy and have grown increasingly familiar with cyber monitoring laws and widely discuss changes to those laws in their own internet forums.”[88] The threat is clearly not just spam or spyware from cybercriminals, but insidious cyber espionage and cyberattacks from nation-state and non-state adversaries.

Conclusion

Though more liberal societies may resist excessive monitoring and control, it may eventually become necessary to forgo complete anonymity and privacy in order to access or connect to certain areas of cyberspace with a level of trust and security commensurate with user expectations. The evolution of these norms of behavior also transforms the ability to detect and respond to cybercrime, cyber espionage and cyberattack, but law and doctrine will always lag behind current application of theory. Michael Schmitt offers the most widely acknowledged normative framework for determining acts of cyberwar depending on severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[89] To maintain legitimacy in the court of world opinion, cyberattack must also conform to *jus in bello* based on established LOAC as influenced by law, doctrine, and ethics.

[88] Marc Jamison, “Sanctuaries: A Strategic Reality, an Operational Challenge” (Strategy Research Project, US Army War College, 2008), 13.

[89] Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *The Columbia Journal of Transnational Law 37* (1999): 885-937.

Chapter 3

Applying the Law of Armed Conflict to Cyberwarfare

No one has yet defined what would constitute an act of war in cyberspace.

-- *United States Air Force General Victor E. "Gene" Renuart Jr.*

On the surface, it appears that the "law of armed conflict [LOAC] provides a reasonable starting point for an international legal regime to govern cyberattack. However, those legal constructs fail to account for non-state actors and for the technical characteristics of some cyberattacks."[1] In fact, nearly every norm of behavior in cyberspace defies a simple application of the LOAC principles of military necessity, humanity, proportionality, distinction, chivalry, and neutrality. Anonymity and connectivity blur the line between valid and invalid targets, while security and control may hamper effects assessment and proportional measurement of response. Susan Brenner states, "Most scholars have concluded that a cyberattack does *not* constitute an act of warfare under the United Nations Charter or other international agreements unless it is accompanied by the use or threatened use of physical force."[2] Nevertheless, some jurists have determined that "cyber attacks could clearly be considered a new weapon if they were used to cause physical destruction in the way bombs do today."[3] Some have even proposed that the international community "develop a declaratory policy on criteria to categorize computer network attacks as a use of force under international law."[4] If cyberattack is a new weapon, the Geneva Conventions require that nations determine whether employment in armed conflict would be prohibited under international law.[5]

[1] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, eds. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Committee on Offensive Information Warfare, (Washington, DC: The National Academies Press, 2009), 5.

[2] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York, NY: Oxford University Press, 2009), 104.

[3] Wolfgang McGavran, "Intended Consequences: Regulating Cyber Attacks," *Tulane Journal of Technology and Intellectual Property 12*, (Fall 2009): 259-275.

[4] House, *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Testimony before the Committee on Foreign Affairs*, 10 March 2010, 8.

[5] Geneva Conference, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, Article 36.

The international community may still be years away from truly operationalizing cyberwarfare. Martin Libicki notes that before a device or technique can be considered weaponized, multiple hurdles must be surmounted:

- Command and control
- Predictable effects and collateral damage
- Conformance with recognizable norms of conduct
- Deployability in time and space
- Integration into combined arms
- Safety in storage and use
- Integrated logistics support
- Training[6]

The United States is overcoming these hurdles rapidly in cyberspace, and the law of armed conflict provides a solid basis for establishing recognizable norms of conduct. Obviously the law "work[s] best when there is some degree of understanding and respect between belligerents."[7] Currently there is no consensus on what constitutes an act of war in cyberspace, nor are there definitive customary or treaty limits to cyber operations in war or peace. Yet, as Libicki quips, "At the end of the day, the answer to whether a particular attack is an act of war comes down to this: Is it in your interest to declare it so?"[8] The Department of Defense has stated that whether a state of conflict exists or not, for information operations, LOAC "is probably the single area of international law in which current legal obligations can be applied with the greatest confidence," and it is in the United States' national interest to remain within this law to maintain legitimacy.[9] It is important to note that LOAC and the norms of behavior in cyberspace "are socially-constructed values that have evolved gradually over time," and that they are subject to interpretation, unique situational application, and most of all—change.[10]

[6] Martin Libicki, *Conquest in Cyberspace* (New York, NY: Cambridge University Press, 2007), 95.

[7] *The Oxford Companion to Military History*, s.v. "laws of war," ed. Richard Holmes et al. (Oxford, England: Oxford University Press, 2001), 493-6.

[8] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND corporation, 2009), 180.

[9] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, May 1999), 11.

[10] Marcelo Halpern and Ajay K. Mehrota, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age," *University of Pennsylvania Journal of International Economic Law 21,* (Fall 2007): 523-561.

The capability to attribute an attack to a specific individual or group is central to determining whether a nation-state response is necessary or even possible. Thus, "one of the distinguishing features between the different types of attacks is whether the attacker is a private citizen or acting at the direction of a government. This distinction is critical because it determines which body of law controls any subsequent response."[11] If an attack is perpetrated by a private citizen, domestic and international law enforcement are implemented, while a state-sponsored attack may be subject to a military response and the law of armed conflict. The dichotomy between the civilian reaction to internal or external crime and a military reprisal for an act of war is problematic in cyberspace for several reasons. Brenner identifies a few in *Cyberthreats*:

- Determining if a cyberattack "comes from" a nation-state can be difficult
- Nation-state "involvement" in an attack is no longer synonymous with war
- The fact that an attack originates *outside* the territory of a particular nation-state does not necessarily mean the state is not sponsoring the attack[12]

Yet even with definitive attribution, "in many ways, the Internet is the perfect platform for plausible deniability."[13] A nation-state can always disavow affiliation with a cyberattack, despite every real or perceived connection, due to the ambiguity caused by anonymity. To date, no state has taken responsibility for any cyberattack, in spite of repeated intrusions worldwide that are strongly suspected to be state-sponsored. It is in our national interest, because of the instantaneous nature of the threat and the extent of our vulnerability that we "initially presume any cyber attack on the critical infrastructure of the United States is a national security threat rather than a criminal activity," and to apply the law of armed conflict to our response.[14] Likewise, it is in our best interest to discourage the norm of anonymity in cyberspace, as this is the single greatest detractor from applying LOAC to cyberwarfare.

[11] Daniel M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China," *American University International Law Review 17,* (2002): 641-681.

[12] Brenner, *Cyberthreats*, 153-4.

[13] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law 27*, (2009): 192-251.

[14] Sean M. Condron, "Getting it Right: Protecting American Critical Infrastructure in Cyberspace," *Harvard Journal of Law and Technology 20*, (Spring 2007): 404-422.

Military Necessity

In order for the principle of military necessity to be applicable, a cyberspace target must be recognizable as a military objective and operations against it must offer a definite military advantage. Military lawyers have determined that "it is clear that computer networks critical to the functioning of enemy infrastructure systems can be valid military targets under customary international law principles ... provided they make an effective contribution to the adversary's military effort and if their destruction would offer a definite military advantage."[15] Targets of this nature could include: Supervisory Control and Data Acquisition (SCADA) systems on electric, water, and sewage grids; industrial manufacturing and information systems; communications satellites or cables; and of course, military command, control, and computer systems.

Many have derided 'industrial web' targets as immoral and ineffective, but the concept is kept alive by military leaders such as Major General Charles Dunlap Jr.: "Under the law of war, there is nothing inherently wrong with destroying or distorting an adversaries' [sic] communication system."[16] Military lawyers back him up, "a civilian computer system, used either to conduct an attack or to shield an aggressor's attack from discovery, becomes a valid and lawful target when: (1) aggression against critical infrastructure equating to an armed attack has occurred; and (2) the total or partial destruction, capture, or neutralization of the computer system offers the United States or its allies a definite military advantage."[17] The Chinese take this concept even further as they perceive "disruption of these institutions is an important element in demoralizing an adversary and reducing its will to fight, and so the Chinese view it as entirely reasonable to attack financial systems, power generation and transmission facilities, and other elements of critical infrastructure as part of conflict with another nation (whether or not that conflict has become kinetic)."[18] It is in our national interest to encourage a norm of

[15] James P. Terry, "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Conflict: What are the Targeting Constraints?" *Military Law Review 169*, (September 2001): 70-89.

[16] For critiques of area bombing, see A.C. Grayling, *Among the Dead Cities* (New York, NY: Walker & Company, 2006) and Robert A. Pape, *Bombing to Win* (Ithaca, NY: Cornell University Press, 1996); Maj Gen Charles J. Dunlap, Jr., "Towards a Cyberspace Legal Regime in the Twenty-First Century," (speech, Air University 2008 Cyberspace Symposium, Maxwell AFB, AL, 16 July 2008).

[17] Terry, "Lawfulness of Attacking Computer Networks," 70-89.

[18] National Research Council, *Technology, Policy, Law, and Ethics*, 333.

separation between civilian and military systems to mitigate this vulnerability while adhering to the LOAC principle of military necessity.

Another major reason to promote positive separation is that assessment of cyberattack effects can be exceedingly difficult, and "without specific treaties dealing with cyber attacks, nations will likely find themselves floundering in any criminal and forensic investigations that they undertake. The anonymous and cross-border nature of cyber attacks greatly compounds the problem."[19] During a conflict, criminal investigation may not be a factor, but forensic analysis regarding the extent and legality of targets will be applicable. Due to the interconnected nature of cyberspace and the lack of control over some forms of cyberattack (worms, polymorphic malware, etc.) predicting and evaluating effects—offensively or defensively—is often problematic. If a commander cannot reasonably determine whether cyberattacks will affect systems or personnel beyond a designated target, or even who to target in response to a cyberattack, it is unlikely attacks or counterattacks will be authorized.[20] Clearly delineating civilian and military cyberspace would separate legitimate targets and delegitimize attacks against critical infrastructure. This would also aid in discriminating combatants and noncombatants, as described in the section on target distinction. While procuring single-use assets may incur considerable cost, those who fail to do so are essentially hiding behind civilians and are accepting the responsibility for collateral damage as limited by humanity and proportionality.

Humanity

Many proponents of cyberattack extol the potential for neutralizing a target without the loss of life or destruction of physical infrastructure. For instance, the National Research Council has stated, "If [an electric] grid's control centers are bombed, it may take a very long time to restore service when the war is over, but if they can be shut down by cyberattacks, it may be possible to restore service much more quickly. The military gain is achieved even by a short-term disruption," so a cyberattack is both more

[19] McGavran, "Intended Consequences," 259-275.

[20] This was the case in the buildup to Iraqi Freedom, when officials cancelled attacks on Saddam Hussein's financial accounts due to fears of collateral damage. See John Markoff and Thom Shankar, "Halted '03 Iraq Plan Illustrates US Fear of Cyberwar Risk," *New York Times*, 1 August 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=1 (accessed 1 April 2010).

humane, and more effective in the long-term due to our propensity for rebuilding a nation once we have defeated the enemy.[21] One must be careful to stay within the principle of military necessity when conducting this type of attack, however.

Cyberattacks on SCADA systems can escalate to a crime against humanity if they produce extensive superfluous suffering. Cutting off electricity, water, and sewage services for an extended period of time may result in death and disease across a large portion of the population. Libicki denigrates the efficacy of cyberattacks, "Nuclear war creates firestorms, destroying people and things for miles around. By contrast, even a successful widespread information attack has more the character of a snowstorm."[22] However, even a much anticipated snowstorm or hurricane can cause extensive deprivation to those who have made reasonable preparations. An unprepared and overwhelmed populace could plausibly succumb to a massive, well-planned cyberattack. It is in our national interest to unilaterally disavow pervasive, long-term SCADA attacks and discourage others from exploring the possibility through the institution of new LOAC limitations against such war crimes.

A different type of cyberattack that may violate the principle of humanity is corruption or exploitation of personal, financial, or familial data. Davis Brown discourages this form of attack: "Disrupting the personal finances or invading the personal privacy of military members assaults them not in their combatant capacities, but in their personal capacities."[23] He classifies this as an outrage to personal dignity which is specifically outlawed by common Article 3 of the Geneva Conventions. This may be stretching the limits of credulity, but it is conceivable that such psychological attacks against civilians could be construed as a crime against humanity, especially if the operation is widespread and permanently damages the livelihood of the victims.

Proportionality

Collateral damage estimates have become a vital part of military planning, but "predicting and understanding the actual outcome of a cyberattack is very intelligence-intensive ... The possibility of false claims exists with kinetic attacks as well, but claims

[21] National Research Council, *Technology, Policy, Law, and Ethics*, 264.
[22] Libicki, *Conquest in Cyberspace*, 39.
[23] Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict," *Harvard International Law Journal 47 no. 1*, (Winter 2006): 179-221.

about collateral damage from a cyberattack are likely to be even more difficult to refute."[24] Thus commanders must be cognizant of not only the potential *actual* effects of a cyberattack, but of the probable *claims* of an unscrupulous enemy. They must weigh the possibility of real or perceived collateral damage against the predicted advantage of the cyberattack, and "if the necessity of the counter-attack were to outweigh the harm resulting from it, then the possibility—even likelihood—that innocent parties' systems may be affected would figure little in the equation. LOAC does not protect noncombatants from being inconvenienced; it protects them only from life-threatening conditions caused by the armed conflict. If innocent parties are harmed in the counter-attack, the responsibility for that harm would lie with the original attacking party who co-opted the innocent systems in the first place."[25] However, recent conflicts have significantly decreased the acceptable level of risk for collateral damage—real or perceived—that commanders are willing to bear.

Even when a target is declared a military objective, commanders are not absolved from restraint. Proportionality also prohibits the use of indiscriminate weapons and attacks which are disproportionate to the offense. Thus disabling the electric power grid of a nation-state or unleashing a virus that infects and destroys every computer connected to a given server simply to interrupt a distributed denial of service attack would violate proportionality. Collateral damage in this case outweighs the advantage gained by neutralizing the avenue of attack. This is one argument against the use of an active defense which responds automatically to rule-based stimuli: the risk of false positives is often excessive, and the potential for reprisal against the merely curious rather than the truly malignant can be too high a price to pay. An active defense may also violate the principle of distinction unless it is strictly monitored.

Some authors have argued that "a passive defense against [Information Warfare] will not work.... Even a single vulnerability given enough 'free' attempts will compromise the system.... Therefore, an active defense in which the attacker is forced to pay a price for targeting a system is paramount."[26] Though the restraints on proportionality are somewhat abated on the defensive compared to collateral damage

[24] National Research Council, *Technology, Policy, Law, and Ethics*, 262-4.
[25] Brown, "Proposal for an International Convention," 179-221.
[26] Shackelford, "From Nuclear War to Net War," 192-251.

restrictions on offensive operations, reprisals are still limited to the requirements of military necessity. If the attacking computers are merely zombies associated with a botnet, then an active defense disabling these computers will harm innocent lives with little effect on the real enemy. A proportional response would involve a concerted effort to track the attack back to the controlling computer before unleashing a counterattack. Yet even the best active systems can be thwarted by anonymizers, so a valid solution is to institute norms against the use of anonymizing tools such as TOR, I2P, and remailers.

Another problem with judging a proportional response is measuring the level of damage from a cyberattack. Cyberattacks are designed to be insidious so they resemble normal traffic until, and even after, the objective has been attained; therefore, detecting and evaluating cyberattack effects is a daunting task—both offensively and defensively. Assessing the extent of the damage, however, could be critical to mounting a proportional response. "If the international community were persuaded that a particular computer network attack or a pattern of such attacks should be considered to be an 'armed attack,' or equivalent to an armed attack, it would seem to follow that the victim nation would be entitled to respond in self-defense either by computer network attack or by traditional military means in order to disable the equipment and personnel that were used to mount the offending attack."[27] The United States and Russia have both declared cyberattacks equivalent to physical attacks, with Russia going so far as to say they are "comparable to that of weapons of mass destruction."[28] Clearly, this raises the potential level of proportional response to the extreme, but the problem of differentiating between actual malicious entities and their unintentional minions remains.

Distinction

According to the Hague Convention, a lawful combatant must: be commanded by a person responsible for his subordinates; have a fixed distinctive emblem recognizable at a distance; carry arms openly; and conduct their operations in accordance with the laws

[27] This is often referred to as the principle of equivalent effects, and is most applicable to making a *jus ad bellum* determination of whether physical attack is appropriate in response to a cyberattack. Department of Defense, *Assessment of International Legal Issues in Information Operations*, 18.

[28] Presidential Decision Directive /NSC-63, Critical Infrastructure Protection, 22 May 1998; Igor Ivanov, Minister for Foreign Affairs of the Russian Federation, to Kofi Annan, United Nations Secretary-General, letter, 20 September 1998.

and customs of war.[29] The norms of anonymity and connectivity in cyberspace complicate target distinction to such a degree that it becomes nearly impossible to determine whether an individual is a combatant or noncombatant, or utilize discriminate weaponry. This situation suggests that "information operations during international armed conflicts be conducted only by members of the armed forces," to avoid any confusion; however, there are others who believe that "cyber attackers forfeit the combatant privilege because they do not identify themselves as combatants."[30] Brown makes a strong argument that "distinction between combatants and noncombatants in information warfare must be scrupulously maintained," so that the civilian population does not become a legitimate target.[31]

While individuals may not be distinguished as combatants, certain physical aspects of cyberspace networks can be identified as strictly civilian. This is because cyberspace is ultimately composed of physically connected networks, managed by rules ordained in software and communications systems—all of which are located within the sovereign boundaries of nation-states.[32] This means nation-states are able to designate certain networks as vital *civilian* assets requiring extra protection. For instance, SCADA systems that govern industrial processes such as water treatment, electrical power transmission, and communications networks have been designated as critical infrastructure and key resources by the Department of Homeland Security in the National Infrastructure Protection Plan.[33] Attacks against these targets can be designated off limits as long as they are not also used by the military.

Unfortunately even if civilian and military communications systems could be singled out for targeting, which is unlikely considering at least 80 percent of military satellite communications are currently transmitted over commercial systems, some assert there is no guarantee that the effects will stay isolated since "even discriminate attacks

[29] Hague Conference, *Regulations Respecting the Laws and Customs of War on Land (Hague II)*, 29 July 1899, Article 1.
[30] Department of Defense, *Assessment of International Legal Issues in Information Operations*, 8; Shackelford, "From Nuclear War to Net War," 192-251.
[31] Brown, "Proposal for an International Convention," 179-221.
[32] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 11-12.
[33] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Government Printing Office, 2009), 12.

easily become indiscriminate because the Internet is interconnected."[34] Yet Microsoft's take-down of the *Waledec* botnet and Spanish authorities' disruption of the *Mariposa* botnet prove that defeating individual cyberattackers is possible.[35] These operations were accomplished by multinational corporations, ad hoc working groups, and domestic law enforcement agencies, but they demonstrate the capability of detecting and neutralizing specific command and control networks without disturbing cyberspace as a whole.

These actions are also indicative of the blurring lines between civilian, law enforcement, and (potentially) military personnel. Susan Brenner postulates that cyberwarfare "will deviate from our expectations by eroding, if not erasing, the noncombatant-combatant distinction that is a fundamental premise of the evolved twentieth-century conception of warfare."[36] This assumes that the international community continues to accept the norm that entities can commit attacks anonymously in cyberspace without repercussion and that individuals and groups online are responsible for their own protection. However to stay within the LOAC principle of distinction it is incumbent upon attackers and defenders alike to separate combatants from noncombatants both physically and in cyberspace, and to provide for their defense.

Chivalry

Chivalry allows lawful ruses but not perfidy. Providing an enemy with misleading information about the location and status of forces through a blog post or by direct manipulation of their information systems would be permissible, but sending a virus attached to an email offering terms of a peace settlement would not. At the same time camouflage is authorized, so a Trojan worm is a lawful weapon as long as it is not disguised as a protected item, such as a message from the International Committee of the Red Cross. Some authors have suggested that misrepresenting other highly recognizable

[34] Andrea Shalal-Esa, "US Military Sees Rising Demand for Satellites," *Reuters*, 2 June 2008, http://www.reuters.com/article/idUSN0229389520080602 (accessed 1 April 2010); Shackelford, "From Nuclear War to Net War," 192-251.

[35] Lance Whitney, "With Legal Nod, Microsoft ambushes Waledac Botnet," *CNET news*, 25 February 2010, http://news.cnet.com/8301-1009_3-10459558-83.html (accessed 24 March 2010); Robert McMillan, "Spanish Police Take Down Massive Mariposa Botnet," *Networkworld* , 2 March 2010, (accessed 24 March 2010) http://www.networkworld.com/news/2010/030310-spanish-police-take-down-massive.html .

[36] Brenner, *Cyberthreats*, 242.

entities such as Microsoft Software Support may constitute perfidy, but there are few who would support this argument.[37]

Misusing internationally recognized symbols can also be accomplished in other ways through cyberspace. Davis Brown suggests that morphing images of military sites to resemble protected sites is an act of perfidy, but "morphing an image to make it appear that nothing is there would be a legitimate ruse."[38] Likewise, altering an enemy's data so they accidently attack a hospital or routing attacks through a protected commercial server may constitute perfidy, but overwhelming the enemy with data so they cannot discern your location or disguising an Internet protocol address as an innocuous civilian may be allowed.

Following the principle of chivalry reinforces the norm of trust, because belligerents should have faith that protected symbols remain sacrosanct. However it exploits the norms of access and connectivity, because it takes advantage of an enemy's credulity and the availability of information. Chivalry could be abused through the norm of anonymity, but ruses depend on it.

Neutrality

According to the Hague Conventions, the use of communications equipment (wireless telegraphy) through a neutral territory is not forbidden as long as the service is provided impartially to all belligerents, however using installations for purely military purposes is prohibited.[39] Since most of cyberspace is dual-use, then practically any cyberattack through a neutral territory is legally authorized as long as the service is not specifically established for military reasons or restricted to one side or another. For all practical purposes, however, it may be impossible to avoid the use of neutral servers due to the distributed connectivity of cyberspace and the uncontrollable nature of autonomous routing protocols.

Another point of view on the principle of neutrality is that state responsibility applies even while a nation-state is neutral. State responsibility holds that a nation-state

[37] Mark Shulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law 37 (Notes)*, (1999): 939-968.
[38] Brown, "Proposal for an International Convention," 179-221.
[39] Hague Conference, *Convention Respecting Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V),* 18 October 1907, Articles 3, 8 and 9.

can be held accountable for attacks coming from its sovereign territory. If attacks are perpetrated from neutral sovereign territory, it is incumbent upon that nation-state to make a concerted effort to stop the attacks or expel the belligerent.[40] Under a state of necessity, a victim of cyberattacks "may take such actions as are necessary in the territory of a neutral that is unable (or perhaps unwilling) to counter enemy IW force activities."[41] Thus a belligerent is within its rights to pursue an enemy on or through neutral territory (i.e., neutral Internet servers) if necessary. This principle is complicated by the ambiguous nature of sovereignty in cyberspace.

Conclusion

To act in accordance with LOAC in cyberspace, customs and practices must be advanced that distinguish legitimate cyberspace combatants, limit collateral effects on critical civilian infrastructure, respect neutral territory and protected entities, and enhance assessment tools used to gauge cyberattack effects. These proposals mirror many of the tenets contained in a seminal *Harvard International Law Journal* article written by Davis Brown, in which he proposed a Convention extending LOAC to information warfare.[42] Conduct in accordance with LOAC is also in keeping with many of the abiding norms of cyberspace behavior detailed in Chapter Two, with the possible exclusion of anonymity. Practical approaches for promoting and reinforcing these norms is the subject of the next chapter.

[40] Also implied by Hague Conference, *Hague V*, Article 5.

[41] The state of necessity is a principle taken from the law of the sea wherein a belligerent warship remains in neutral territorial waters and the neutral country is unable or unwilling to expel the vessel as LOAC provides. State of necessity can be invoked to preclude wrongfulness of conduct adopted in certain conditions to protect a target state's essential interest, without the third state's existence being in any way threatened. George K. Walker, "Information Warfare and Neutrality," *Vanderbilt Journal of Transnational Law* 33(5), (November 2000):1079-1200.

[42] See Appendix B, *Draft Convention Regulating the Use of Information Systems in Armed Conflict*.

Chapter 4

Influencing Cyber Norms of Behavior

> *The theory of hegemonic stability posits that the leader or hegemon facilitates international cooperation and prevents defection from the rules of the regime through use of side payments (bribes), sanctions, and/or other means but can seldom, if ever, coerce reluctant states to obey the rules.*
>
> -- *Robert Gilpin*

The capacity to influence norms of behavior has also been called soft power by Joseph Nye and friendly conquest by Martin Libicki. In short, soft power is "the ability to get what you want through attraction rather than coercion and payments" and friendly conquest involves establishing a useful, assured system so that "users may find themselves not only growing dependent on it, but deepening their dependence on it by adopting standards and protocols for their own systems."[1] While many neorealists, such as Kenneth Waltz, Robert Kagan and Robert Gilpin, and neoliberals, such as Robert Keohane, discount the sociological efficacy of soft power, the idea has had appeal since the age of Lao Tzu and Thucydides.[2] The power of normative influence is best described in the tenets of social constructivism espoused by international relations theorists such as Alexander Wendt and Peter Katzenstein.[3] A central principle of this theory is that "states may not always know what they want and are receptive to teaching about what are appropriate and useful actions to take" based on social and cultural factors and a sense of collective identity manifested in international organizations.[4]

[1] Joseph Nye Jr., *Soft Power: the Means to Success in World Politics* (New York, NY: Public Affairs, 2004), x; Martin Libicki, *Conquest in Cyberspace* (New York, NY: Cambridge University Press, 2007), 12.

[2] For treatises on structural realism see Kenneth Waltz, *Theory of International Politics* (New York, NY: McGraw Hill, 1979) and Robert Kagan, *Of Paradise and Power: America and Europe in the New World Order* (New York, NY: Vintage, 2004) an economic view is presented by Robert Gilpin in *Global Policital Economy*; the insights of neoliberalism can be found in Robert Keohane, *After Hegemony* (Princeton, NJ: Princeton University Press, 1984); for the appeal of soft power see Lao Tzu, *Tao Te Ching* ed. and trans. Jonathan Star (New York, NY: Penguin, 2001) and Pericles' Funeral Oration in Robert B. Strassler, *The Landmark Thucydides* (New York, NY: Simon & Schuster, 1996), 2.34.8-2.46.

[3] Alexander Wendt, *Social Theory of International Politics* (Cambridge, UK: Cambridge University Press, 1999); Peter Katzenstein, ed., *The Culture of National Security: Norms and Identity in World Politics* (New York, NY: Columbia University Press, 1996).

[4] Martha Finnemore, *National Interests in International Society* (Ithaca, NY: Cornell University Press, 1996), 11.

There are many ways in which norms of behavior can emerge. Katzenstein offers four: spontaneously evolving, as social practice; consciously promoted, as political strategies to further specific interests; deliberately negotiated, as a mechanism for conflict management; or as a combination of the three preceding types.[5] Martha Finnemore and Kathryn Sikkink describe a three-stage life cycle of norm development from initial emergence through a widening cascade to eventual internalization. They suggest norms can reach a tipping point caused by a multitude of factors: legitimacy of the entity adopting the emerging norm; prominence of the entity introducing the norm; intrinsic qualities of the norm; adjacency of the new norm to an existing norm; and 'world time' or current events favoring the norm.[6] Finnemore further suggests that "state interests are defined in the context of internationally held norms and understandings about what is good and appropriate. That normative context influences the behavior of decisionmakers and of mass publics who may choose and constrain those decisionmakers. The normative context also changes over time, and as internationally held norms and values change, they create coordinated shifts in state interests and behavior across the system."[7] Thus international norms of behavior alter, and are altered by, the balance of power.

In the final analysis, a consensus of the majority establishes norms of behavior, but a powerful minority can influence their choices. Thus the traditional realist incentives of fear, honor, and interest in a coercive, anarchic system are combined with the liberal ideals of prestige and complex interdependence in an environment of international cooperation to produce a sociological theory in which "security interests are defined by actors who respond to cultural factors."[8] Influencing and exploiting cyber norms of behavior to promote ethical and moral conduct will exercise all elements of national power, and as Katzenstein implies, a united minority can consciously promote and deliberately negotiate these norms to generate concurrence of the international majority.

[5] Peter Katzenstein, "Introduction: Alternative Perspectives on National Security," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter Katzenstein (New York, NY: Columbia University Press, 1996), 21.

[6] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887-917.

[7] Martha Finnemore, *National Interests in International Society*, 2.

[8] Peter Katzenstein, "Introduction: Alternative Perspectives on National Security," 2.

Crafting Cyber Norms

Ever since the United States created the Internet in the 1970s through investments in the Defense Advanced Research Project Agency, it has retained considerable authority over the growth and structure of cyberspace through organizations such the Internet Corporation for Assigned Names and Numbers (ICANN).[9] Many of the principal computer networking engineers and telecommunications companies have been American, and they exerted substantial influence in the international consortia that guided cyberspace development. In recent years, however, that monopoly has been diminishing as other nations cultivate their cyber expertise.[10] One of the challenges America and its allies face is how to retain control over this dynamic source of social, political, and economic power while advancing the freedoms that will allow it to mature to its fullest potential.

The Internet Engineering Task Force (IETF), founded in 1986, made an early attempt to define the future of Internet standards, and became the model for a bottom-up approach to proto-government.[11] However, traditional national governments, particularly the United States, soon exerted their influence on the rules and bodies governing the Internet. They did this primarily through political pressure on local intermediaries, such as Internet Service Providers and communications companies, though the United States held considerable sway in the IETF and other budding ad hoc Internet associations because most of the engineers, vendors, and researchers were American. Nation-states, nongovernmental organizations, and multinational corporations all understand that "control over the Internet's standards is how network norms are created."[12] These standards include software formatting such as Transmission Control Protocol (TCP), Internet Protocol (IP), and HyperText Transfer Protocol (HTTP) that form the structure of content and communications through cyberspace, as well as router and server

[9] Harold Kwalwasser, "Internet Governance," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 500.

[10] Kwalwasser, "Internet Governance," 524.

[11] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York, NY: Oxford University Press, 2006), 24; IETF can be found at http://www.ietf.org/.

[12] Goldsmith and Wu, *Who Controls the Internet?*, 102.

configurations that provide the hardware platform for the Internet.[13] Intimate involvement in deciding how these standards are developed and implemented provides a significant influence over the norms of behavior in cyberspace.

Another avenue for manipulating the cyberspace environment indirectly is through telecommunications and economic regulations. By defining legal and illegal activity, nation-states set boundaries on acceptable behavior and execute penalties for exceeding those limits. Requiring financial and federal institutions to establish computer security programs through domestic laws such as the Computer Fraud and Abuse Act is a good first step, but to appreciably deter cyberattacks it will be necessary to integrate and standardize law enforcement through international cooperation initiatives such as the Convention on Cybercrime. Only the combined power of nation-states and a united application of force will change the behavior of cyberspace users.

A truly collaborative effort will entail aligning the interests of the international community, which has been the holy grail of the United Nations since its inauguration. This prototypical international confederation has facilitated cooperation pursuing noble goals from collective security to economic development, environmental sustainability to disease control, and human rights to world peace, but its ultimate authority rests in the sovereign equality and accountability of its member states. Attaining progress towards cyberspace governance will depend on defining sovereignty and state responsibility in this new domain. The United Nations or similar international organization may provide a platform for influencing cyberspace norms to this end.

Internet Architecture and Security Measures

Martin Libicki explains the advantage of devising a standard: "Dominant systems can set the rules and make it harder to justify establishing systems based on competing one."[14] In other words, the pioneer usually has a disproportionate influence on the resulting norms. This is not to say that norms are the sole creation of a dominant power. "By allowing a greater amount of participation by affected organizations and individuals, a stronger argument can be made that any agreement reflects an agreed upon behavioral

[13] These protocols are maintained by the Internet Assigned Numbers Authority (http://www.iana.org/) which is run by the Internet Corporation for Assigned Names and Numbers (http://www.icann.org/).
[14] Libicki, *Conquest in Cyberspace*, 13.

norm for [Information Warfare]. As such, it can be viewed as creating a legal obligation for participants, which should lead to a more rapid acknowledgement of its role as customary international law."[15] Involving a wider range of contributors in development of a more secure Internet architecture will ease the acceptance of a paradigm, though it may complicate the prospect for consensus. "Collecting and publishing best practices for security and threat management from constituent organizations, sharing and monitoring data, championing research efforts, and assisting with response activities during times of crisis" are positive measures that responsible actors can take to mitigate the threat of cyberattack and encourage ethical and moral conduct in cyberspace.[16]

It has often been suggested in the international community that the United States retains undue influence over the standards and protocols that form the underlying structure of cyberspace. "Partially in response to its critics, the United States transferred control of the root to the Internet Corporation for Assigned Names and Numbers (ICANN), a semi-private, nonprofit organization based out of California," however this was insufficient for many because it was still considered an American-run company.[17] "While some governments attempted to reform ICANN, others suggested that responsibility for the root should be transferred to an international organization."[18] One of the prime candidates for this responsibility is the International Telecommunications Union (ITU), which is currently part of the United Nations. "ICANN has evolved as a byproduct of the collision between geographically bounded trademark law and the limitless reach of the Internet," but the ITU is a respected arbiter of telecommunication disputes with over a century of experience.[19] Though it may result in the loss of some control, it is in the United States' interest to help establish an internationally accepted Internet governing body to maintain the legitimacy of any decisions on global standards.

[15] Jon P. Jurich, "Cyberwar and Customary International Law," *Chicago Journal of International Law 9,* no. 1 (Summer 2008): 275-294.

[16] Abraham M. Denmark et al. eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security Report, January 2010, (accessed 12 February 2010), 37 http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.

[17] Scott P. Sonbuchner, "Master Your Domain: Should the U.S. Government Maintain Control over the Internet's Root?" *Minnesota Journal of International Law 17,* (Winter 2008): 183-207.

[18] Sonbuchner, "Master Your Domain," 183-207.

[19] Marcelo Halpern and Ajay K. Mehrota, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age," *University of Pennsylvania Journal of International Economic Law 21,* (Fall 2007): 523-561.

Yet despite a general acceptance that international cooperation is necessary, especially in the realm of cyber security, "unilateral action, conflict, and ad hoc accommodation are often the best the nations of the world can do."[20] This is because "the international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt."[21] Architecture changes and international security agreements to restrict cyberattacks may not happen until they are seen as a credible threat to national security or economic well-being. This threshold is rapidly approaching, and the potential for influencing cyber norms will depend on strong American diplomatic and economic support for a more secure Internet architecture.

Another rapidly approaching threshold is the limit on IP addresses imposed by the current architecture, IPv4. The American Registry for Internet Numbers estimates there is less than 10% of 32-bit address space left, and the remaining addresses will be gone by late 2011.[22] The newest iteration of Internet protocol architecture, IPv6, has 128-bit hexadecimal addressing and makes Internet Protocol Security mandatory (among other improvements), but despite its deployment more than a decade ago, it has not earned widespread acceptance. This is due in part to the daunting costs and work load involved in making the conversion, but in order for the Internet to grow the change must be made. This is another example of the international community waiting for a crisis in order to act, but executing this transformation offers an opportunity to influence norms of behavior concerning security and control, though it poses significant challenges as well.[23]

Independent organizations are already pursuing other technological advances to increase the underlying security of Internet architecture. The computer emergency response team at Carnegie-Mellon has been working on the LEVANT (Levels of Anonymity and Traceability) project for a number of years in an attempt to build trust

[20] Goldsmith and Wu, *Who Controls the Internet?*, 167.

[21] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, May 1999), 2.

[22] American Registry for Internet Numbers, "IPv4/IPv6: The Bottom Line," (accessed 2 April 2010) https://www.arin.net/knowledge/v4-v6.html. An actual counter for the remaining address space can be found at http://www.inetcore.com/project/ipv4ec/index_en.html.

[23] For an extensive look at the challenges of switching to IPv6, see Sheila Frankel, Richard Graveman, and John Pearce, *Guidelines for the Secure Deployment of IPv6 (draft)* (Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Division, February 2010), Special Publication 800-119.

networks and balance the conflicting needs of privacy and security.[24] There is an entire universe of host-based and network-based security systems designed to protect information systems that is beyond the scope of this paper, but it is sufficient to mention that for the foreseeable future if a network is connected to the wider Internet, it cannot ever be completely secure.

In the quest for cyberspace control, "states are only one of many actors who seek to invoke the existence of international legal norms."[25] Nongovernmental organizations, multilateral corporations, and other non-state entities have an increasing power to influence majority consensus based on successful business models, pervasive software and hardware brands, and growing dependence on certain social and business networking tools. Examples such as the dominant Microsoft Office, Apple iPod, and emerging giants Google, Facebook, and Twitter abound. It may be necessary to include these actors in the actual decision-making process of an international cyberspace governing body, as is currently done at ICANN, or at a minimum provide them access for suggestions. At present however, implementing and enforcing standards through legal and political means can only be accomplished through the enforcement of domestic law.

International Law and Cooperation

Generally law lags experience, so the lack of coherent cyber law should not be a surprise. Analysts at the North Atlantic Treaty Organization (NATO) suggest "one possible explanation for the lack of a coherent international legal framework governing cyberspace is that great power states such as the U.S., China, and Russia may desire a significant degree of strategic ambiguity while they shape their own national cyber based military capabilities. Another possible explanation is that too few diplomats and legislators lack the requisite technical expertise to comprehend fully the scope of cyber defence issues."[26] To rectify the perceived vulnerabilities highlighted by the Estonia cyberattacks in 2007, NATO developed a cyber defense policy and opened the

[24] Computer Emergency Response Team, "LEVANT," 3 May 2007, http://www.cert.org/sse/levant.html (accessed 2 April 2010).

[25] Andreas L. Paulus, "Commentary to Andreas Fischer-Lescano & Gunther Teubner: The Legitimacy of International Law and the Role of the State," *Michigan Journal of International Law 25*, (Summer 2004): 1047-1058.

[26] Rex B. Hughes, "NATO and Cyber Defence," *Atlantisch Perspectief 8*, 2008 (accessed 19 March 2010) http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia in 2008. The Partnership for Peace Information Management System established in 1996 to facilitate collaboration and interoperability is another example of positive international cooperation for cyber security.[27]

The most significant effort to deal with the problem of cyber security, however, is the Council of Europe's Convention on Cybercrime. Unfortunately this treaty has had a tepid response, and even if it were ratified universally "it is likely that some gray area will always exist between LOAC and criminal law when certain kinds of cyberattack occur."[28] The norm of anonymity forms a substantial barrier in the battle against cyberattacks. This is not to imply the potential threat is insurmountable. As former Deputy Judge Advocate General for the Air Force, Major General Charles Dunlap Jr., has said, "While I am not keen on seeking to revise the law of war, per se, it may be the right time to consider strengthening the international legal norms related to cyber activities, especially those applicable in peacetime."[29]

Many jurists are not convinced that international law is the solution, because "the main problem does not lie in the international legal requirements for binding norms, but in the limitations of its law-making subjects to States.... non-state actors can only bind themselves."[30] International law is weakly enforced even for nation-states, and for non-state actors it is virtually nonexistent. Another limitation is shown in disparate cultural values, which can be magnified due to the connectivity of cyberspace and that defy universal reconciliation. "International treaties with subtle legal points cannot satisfy the common sense functionalism of the Internet, nor can they appeal intuitively across cultural borders. Likewise, judicial decisions, based on the diverse legal processes of different jurisdictions, can only resolve momentary tensions of conflicts."[31] This may

[27] Cooperative Cyber Defence Centre of Excellence can be found at http://www.ccdcoe.org/; Partnership for Peace Information Management System can be found at http://www.pims.org/.

[28] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, eds. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Committee on Offensive Information Warfare, (Washington, DC: The National Academies Press, 2009), 34.

[29] Maj Gen Charles J. Dunlap, Jr., "Towards a Cyberspace Legal Regime in the Twenty-First Century," (speech, Air University 2008 Cyberspace Symposium, Maxwell AFB, AL, 16 July 2008).

[30] Andreas L. Paulus, "Commentary to Andreas Fischer-Lescano & Gunther Teubner," 1047-1058.

[31] Halpern and Mehrota, "From International Treaties to Internet Norms," 523-561.

become less of a problem as sovereignty takes shape in cyberspace, or as social norms merge in the increasingly networked world of cyberspace.

Social Media and Information Management

The use and proliferation of social networking systems, blogs, wikis and other collaborative Web 2.0 applications is one of the most powerful modern influences on cyber norms of behavior. The ease of access and connectivity provided by these services enables a speed of global information transfer that was unheard of a decade ago. To gauge the rapid advancement of these technologies, consider the incorporation dates of the top five websites we now take for granted, in order of popularity.[32]

Google	1998 (IPO 2004)
Facebook	2006
YouTube	2005
Yahoo	1995
Live	2005

Of the next six (Wikipedia, Baidu, Blogger, msn, qq, and Twitter) only one was created before 1999, and two are almost exclusively Chinese. Traditionally conservative government agencies have had difficulty keeping pace with the growth of these systems. Air Force Public Affairs has issued a guide to using social media that states: "In the past, the Air Force did not officially engage blogs or other forms of social media. Now, Air Force leaders realize the broad reach—both positive and negative—these forms of communication have on Airmen and society, as well as the value of maintaining a presence in this information domain."[33] After over a decade of limiting access and enforcing strict controls on computer usage, the military is starting to realize the power of connectivity while maintaining extensive monitoring for security purposes.

In June 2009, Army Operations Order 09-01 opened the flood gates to social media for troops. The Air Force followed suit with Air Force Guidance Memorandum to AFI 33-129, *Web Management and Internet Use*, in accordance with Directive-Type Memorandum 09-026, *Responsible and Effective Use of Internet-based Capabilities*,

[32] According to Alexa, "Top Sites," http://www.alexa.com/topsites (accessed 5 May 2010).

[33] Air Force Public Affairs Agency, *Social Media and the Air Force* version 2, (Arlington, VA: Emerging Technology Division, November 2009), 1.

signed on February 25, 2010. This means certain government computers are now allowed access to social media and networking websites such as Facebook, YouTube, Twitter, and Flickr within specific rules of engagement guided by the Uniform Code of Military Justice and operations security. "Military leaders are recognizing the importance of social media and taking steps to incorporate change into their organizational cultures."[34] This will inevitably lead to higher risk, but "trust enables leaders to open up their organizations to social media, and training provides confidence in the rules of engagement that govern social media use."[35] Social media are a wellspring for the norms of trust, access and connectivity, but tend to complicate monitoring, control and security. They can also impact privacy depending on the level of anonymity that is maintained. Policy and doctrine concerning the use and usefulness of social media is still in considerable flux.

Encouraging the use of social media will lead to a more open, free exchange of information, which positively influences cyber norms of behavior, and will be an important aspect of advancing both a liberal democratic diplomatic agenda and ensuring successful military operations in the future. Social activism through Twitter and YouTube has been seen in Iran and China, and collaborative websites were also used extensively in the cyberattacks on Estonia and Georgia.[36] United States Joint Forces Command also recognizes the power of collaborative tools to enhance planning, execution, and assessment of more traditional military operations.[37] The potential—positive and negative—of social media services is incredible, and it is imperative that the United States harness the power of these applications to promote its national interests.

Defining and Defending Sovereignty

The concept of sovereignty in cyberspace poses one of the greatest conundrums to

[34] Chondra Perry, "Social Media and the Army," *Military Review*, March-April 2010, 20-32.
[35] Perry, "Social Media and the Army," 20-32.
[36] Jon Leyne, "How Iran's Political Battle is Fought in Cyberspace," *BBC News*, 11 February 2010, http://news.bbc.co.uk/2/hi/8505645.stm (accessed 15 March 2010); Sharon LaFraniere and Jonathan Ansfield, "China Alarmed by Security Threat from Internet," *New York Times*, 11 February 2010, http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html (accessed 16 February 2010); Byron Acohido, "Some Russian PCs Used to Cyberattack Georgia," *USA Today*, 17 August 2008, http://www.usatoday.com/tech/news/computersecurity/hacking/2008-08-17-russia-georgia-war-hackers_N.htm (accessed 5 May 2010).
[37] Gary Luck and Mike Findlay, *Joint Operations Insights and Best Practices* 2nd ed. (Suffolk, VA: USJFCOM Joint Warfighting Center, July 2008), 54.

challenge international governance of cyberspace. Michael Walzer describes political sovereignty as the "independence from foreign control and coercion," but he bases his legalist paradigm on the territorial integrity of independent states.[38] Historically, as Susan Brenner posits, "The most efficient, most effective organizational model was one that centralized power in a single source: the sovereign" whose power was derived from coercive physical force based on legitimately accepted rules.[39] Since the Peace of Westphalia, sovereignty has been consolidated by territorially distinct nation-states. Though anyone can use force—physical, moral, or cyber—Kenneth Waltz states that an effective government "has a monopoly on the *legitimate* use of force."[40] In the early 1990s, the expanded legitimate use of peace-keeping forces for humanitarian assistance seemed to threaten the integrity of national sovereignty, which prompted the United Nations Secretary-General to write: "National boundaries are blurred by advanced communications and global commerce, and by the decisions of States to yield some sovereign prerogatives to larger, common political associations."[41] The transnational nature of cyberspace has further threatened the legitimacy of territorial sovereignty, and the ability of many nation-states to enforce domestic laws regulating Internet usage.

While some believe that "the Internet has broken down many of the geographical and temporal premises of international law," and that "the Internet's great ability to foster globalized free market competition and free speech cuts across traditional geographic boundaries and challenges historic notions of national sovereignty," others believe that "physical coercion by government—the hallmark of a traditional legal system—remains far more important than anyone expected."[42]   Still, attacking or prosecuting individuals located in another country poses significant legal and political challenges. For instance "even if it were possible to conduct a precise computer network attack on the equipment

[38] Michael Walzer, *Just and Unjust Wars* (New York, NY: Basic Books, 1977), 89.

[39] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York, NY: Oxford University Press, 2009), 211-212.

[40] Kenneth N. Waltz, *Theory of International Politics* (Boston, MA: McGraw Hill, 1979), 104.

[41] United Nations General Assembly, Report of the Secretary-General on the Work of the Organization, *An Agenda for Peace: Preventive Diplomacy, Peacemaking and Peacekeeping*, U.N. Doc. A/47/277/S/2411, 17 June 1992, 3. Quoted in Paul Kennedy and George J. Andreopolous, "The Laws of War: Some Concluding Reflections," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard et al. (New Haven, CT: Yale University Press, 1994), 224.

[42] Halpern and Mehrota, "From International Treaties to Internet Norms," 523-561; Kwalwasser, "Internet Governance," 492; Goldsmith and Wu, *Who Controls the Internet?*, 180.

used by such individual actors, the state in which the effects of such an attack were felt, if it became aware of it, could well take the position that its sovereignty and territorial integrity had been violated."[43] This is the primary issue China and Russia have with the Convention on Cybercrime; allowing cross-border inspections by foreign law enforcement agencies infringes on their sovereignty.[44] Article 32 authorizes a Party of the Convention to "access publicly available (open source) stored computer data, regardless of where the data is located geographically."[45] This Article seems odd, since Articles 27, 29 and 30 include specific provisions for refusal to disclose requested data if:

> (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
>
> (b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.[46]

There are two main policies the United States can pursue concerning cyber sovereignty: establish strict state sovereignty based on ownership of hardware within territorial limits; or support an international consortium to secure cyberspace through law collective enforcement. The United Nations seems to favor the latter, as demonstrated by multiple resolutions that stress the importance of a global culture of cyber security.[47] Despite these collaborative sentiments, however, an expert United Nations panel convened in 2005 was unable to arrive at sufficient consensus to provide even a preliminary report of their progress due to "the complexity of the issues involved."[48] Russia and China have expressed their preference for territorial-based sovereignty, but the United States has not declared an official opinion on the subject.

[43] Department of Defense, *Assessment of International Legal Issues in Information Operations*, 22.

[44] John Markoff and Andrew Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, 12 December 2009, http://www.nytimes.com/2009/12/13/science/13cyber.html (accessed 10 February 2010).

[45] Council of Europe, *Convention on Cybercrime* (Budapest, Hungary: European Treaty Series No. 185, 23 November 2001), Article 32a.

[46] Council of Europe, *Convention on Cybercrime*, Articles 27.4, 29.5, and 30.2.

[47] Namely, United Nations General Assembly resolutions which have been promulgated yearly since 1998: 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17 and 63/37.

[48] United Nations General Assembly, Report of the Secretary-General on the Work of the Organization, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/60/202, 5 August 2005, (accessed 17 December 2009) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

Yet the 2009 Cyberspace Policy Review calls for a strategy to shape "norms regarding territorial jurisdiction, sovereign responsibility, and use of force," and supports participation "in regional or other forums to drive common policy objectives."[49] This suggests the United States is also in favor of a territorial-based definition of sovereignty, but is open to international discussion of the matter. Some legalists believe that "as a practical matter, however, concerns over sovereignty should not forestall international action on cyber attacks. It is well established in international law that the effects principle permits the regulation of activities that impact upon a state's territory."[50] The effects principle is also known as state responsibility.

The concept of state responsibility proposes that "every state has an affirmative legal obligation to prevent its territory from being used for attacks on other states."[51] Goldsmith and Wu remind us that "in the late 1990s, there was broad agreement that the Internet's challenge to government's authority would diminish the nation-state's relevance."[52] Yet despite these utopian predictions, nearly twenty years later "state responsibility remains a bastion of international security."[53] One reason for this is the institution of geographical borders on the Internet, which are emerging "not as a result of fiats by national governments, but rather organically, from below, because Internet users around the globe demanded different Internet experiences that corresponded to geography."[54] Since geography is still important in cyberspace, the concepts of state sovereignty and responsibility are still applicable, and nation-state should be held accountable for cyberattacks that originate within its sovereign territory.

Due to the growing territorial barriers on the Internet, "states continue to be the main unit of legitimacy and of, ideally democratic, debate and decision-making," because "many aspects of the Internet that business and individual users take for granted are the

[49] White House, *Cyberspace Policy Review,* May 2009, (accessed 17 December 2009), 20-1. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[50] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law 27*, (2009): 192-251.

[51] Paul Rosenzweig, "National Security Threats in Cyberspace" (workshop report, American Bar Association Standing Committee on Law and National Security, Annapolis, MD, 4-5 June 2009), 14.

[52] Goldsmith and Wu, *Who Controls the Internet?*, 3.

[53] Shackelford, "From Nuclear War to Net War," 192-251.

[54] Goldsmith and Wu, *Who Controls the Internet?*, 49.

product of a stable legal environment that only governments provide."[55] Sovereign nations remain the primary engine of law enforcement, but if an international governing organization is instituted, giving non-state actors a voice may "enhance the acceptance of any formed law in the long-term by incorporating [their] socio-economic interests ... which should generate clearer norms by forcing increased discussion and reaction to these apprehensions."[56] Incorporating non-state organizations in the international decision-making process also improves the norms of trust and connectivity; however, the abiding norm of anonymity still confounds attribution of cyberattacks to a specific nation-state or sub-state entity.

The difficulty of detecting and deterring cyberattacks is put into context by Jack Goldsmith, "Creating norms to curb cyberattacks is difficult enough because the attackers' identities are hard to ascertain. But another large hurdle is the [United States] government's refusal to acknowledge more fully its many offensive cyber activities, or to propose which such activities it might clamp down on in exchange for reciprocal concessions by our adversaries."[57] In other words, two of the major issues that impair discussion about cyberwarfare are the anonymity inherent in cyber activity and the secrecy that shrouds policy and doctrine on all sides. Technical and philosophical approaches to eliminating the norm of anonymity have been addressed, but defining sovereignty and removing the veil of ambiguity surrounding cyberwarfare will require major policy and doctrinal changes at both the national and military level.

Doctrinal Change

Retired U.S. Army Brigadier General Huba Wass de Czege warns, "A balance has to be struck between providing functionality and applying safeguards"[58] to our cyberattack capability. The United States government has taken great strides towards defending cyberspace infrastructure, but open discussion with private industry and the international community about offensive intentions has been lacking, because "too much

[55] Andreas L. Paulus, "Commentary to Andreas Fischer-Lescano & Gunther Teubner," 1047-1058; Goldsmith and Wu, *Who Controls the Internet?*, 118.
[56] Jurich, "Cyberwar and Customary International Law," 275-294.
[57] Jack Goldmith, "Can We Stop the Cyber Arms Race?" *Washington Post*, 1 February 2010, 17.
[58] Huba Wass de Czege, "Winning in the Cyberelectromagnetic Dimension of 'Full Spectrum Operations,'" *Military Review*, March-April 2010, 20-32.

of the debate on policies related to cyber war is happening behind closed doors."[59] Increased transparency of strategic cyber technologies, honest discourse concerning threats and vulnerabilities, and "public revelation of our response doctrine will be to our benefit. Doing so will create international norms for behavior and then, collaterally, attach a stigma to those who fail to conform."[60] In other words, divulging certain offensive cyber capabilities and deterrent intentions to the international community will decrease risk, increase security, and lead to multilateral treaties limiting cyberwarfare based on the law of armed conflict.

For instance, a declaratory policy holding nation-states accountable for cyberattacks conducted from sovereign territory will increase pressure on everyone, especially the United States, to control cyberspace through stricter limitations on anonymity. To ease the issue of attribution, "it should be enough to prove operational control of government in a [cyberattack], rather than complete governmental control."[61] Also a doctrine of no-first-use or widespread attacks on critical civilian infrastructure will set limits on the employment of cyber weaponry and encourage the extension of LOAC to cyberspace. Finally, implementation of tighter monitoring through mandatory Internet Service Provider registration and delegitimizing anonymizers will enhance global Internet security.

National Guidance

According to Colonel Gary Brown, a Staff Judge Advocate with United States Cyber Command, "the United States has not been involved in establishing any limits to cyberattacks in international law."[62] A report from the National Research Council warns that the "United States has much to lose from unrestrained cyberattack capabilities that are proliferated worldwide."[63] While the United States may have a temporary advantage in cyber capabilities, this hegemony will certainly not last. It is in the best interest of the

[59] Paul B. Kurtz, "Virtual Criminology Report 2009" (Santa Clara, CA: McAfee, Good Harbor Consulting, 2009), http://www.mcafee.com/uk/local_content/reports/virtual_criminology_report/vcr_09.html, 3.
[60] Rosenzweig, "National Security Threats in Cyberspace," 19.
[61] Shackelford, "From Nuclear War to Net War," 192-251.
[62] Colonel Gary Brown (Staff Judge Advocate, United States Cyber Command), interview by author, 2 November 2009.
[63] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, eds. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Committee on Offensive Information Warfare, (Washington, DC: The National Academies Press, 2009), 5.

United States to influence norms of behavior so that uncontrolled cyberattacks are not condoned and that any cyberattacks that do occur are guided by LOAC whether a declared state of conflict exists or not.

Rebecca Grant calls 2008 "the year that cyberspace—its vulnerability, its defense, and its exploitation—passed the point of no return as a major issue for national security officials."[64] The formation of United States Cyber Command as a sub-unified command under United States Strategic Command—coordinating the capabilities of the National Security Agency and the JFCC-NW—will go a long way to consolidate the efforts of cyber security experts. To further improve both offensive and defensive capabilities, the United States will require stronger interagency synchronization to develop structures that permit lawfully authorized clandestine cyber intrusions and protections without risk of public disclosure of specific operations or methods.[65] This implies organizations melding the efforts of state and federal law enforcement, Department of Homeland Security, intelligence agencies, and international allies. The legal environment is complicated, because "cyberspace forces may at one moment be operating under Title 10, U.S.C., *Armed Forces*, and another under Title 50, U.S.C., *War and National Defense*. In addition, some cyberspace forces may be operating under Title 32, U.S.C., *National Guard*."[66] This makes military operations in cyberspace exceedingly messy.

Military Doctrine

It seems inconceivable that the modern networked military could operate without free, open, and secure access to cyberspace. The Department of Defense estimates they have as many as seven million computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications, which does not include the recent explosion in unmanned vehicles.[67] In fact Czege says, "conceptually separating what happens daily on the Internet from what happens in [military networks] ignores their connection and would therefore be unrealistic and dangerous."[68] Regardless of the growing reliance on cyberspace, it is critical that "the Pentagon must begin to

[64] Rebecca Grant, "The Cyber Menace," *Airforce-Magazine.com 92, no. 3*. (March 2009) http://www.airforce-magazine.com/MagazineArchive/Pages/2009/March%202009/0309cyber.aspx

[65] Rosenzweig, "National Security Threats in Cyberspace," 22-23.

[66] Air Force Doctrine Document 3-12 (draft), *Cyberspace Operations*, 30.

[67] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 37.

[68] Wass de Czege, "Winning in the Cyberelectromagnetic Dimension," 20-32.

develop technologies and concepts that will allow the military to operate effectively without use of the Internet."[69] As the Commander of United States Strategic Command, General Kevin Chilton, is fond of saying, we must develop Mission-Oriented Protective Posture gear for cyberspace operations, because "the hardest thing is going to be to fight through attacks in the future and ensure that the domain continues to operate in at least an adequate fashion so we can continue operations in every other warfighting domain."[70]

There is no doubt that "the important disciplines of 'operations security' and 'information assurance' must become rigorously foundational habits and a matter of command interest at all levels."[71] Yet despite the apparent desire to make cyberwarfare a central component of military strategy, it remains segregated from other overall planning efforts because of highly compartmented classification.[72] To rectify this problem and elevate the importance of cyberwarfare in exercises and operations, "to the extent possible, discussions about cyber law, doctrine, and policy should not be classified."[73] Cyberwarfare capabilities must be inculcated in military training and education, and become an integral function of operational planning and execution.

A RAND report written to guide the (ultimately cancelled) stand-up of Air Force Cyber Command offered three salient recommendations for future operations:

- improve situational awareness—not only of Air Force networks but also of upstream joint and interagency network activities and of the risks of relying on critical infrastructures shared with commercial partners
- integrate enhanced active responses into network operations (in collaboration with others)
- integrate active cyberspace defenses (and selected offensive cyber capabilities) with kinetic operations in air operations centers[74]

[69] Denmark, *Contested Commons*, 40.

[70] Kevin P. Chilton, (speech, 2009 Cyberspace Symposium, Omaha, NE, 7 April 2009), http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium (accessed 23 March 2010).

[71] Wass de Czege, "Winning in the Cyberelectromagnetic Dimension," 20-32.

[72] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 14.

[73] Rosenzweig, "National Security Threats in Cyberspace," 19.

[74] Richard Mesic et al., "Air Force Cyber Command (Provisional) Decision Support" (RAND report, Santa Monica, CA, 2010), 11.

Czege also suggests we should not separate "the fields of experts who create and operate our advanced networks from the experts who destroy and manipulate the enemy's."[75] There is some evidence that cyber operations are becoming more integrated with kinetic operations, but the military and the rest of the interagency team are still bridging this gap. For instance, the Falconer Air and Space Operations Center has been declared a weapon system and contractors such as Northrup Grumman have developed simulators such as the Cyber Warfare Integration Center to aid in exercises.[76] It is possible that United States Cyber Command will be able bring these elements together, but two important missing items, at least at the unclassified level, are an integrated military strategy and operational rules of engagement which will enable the ethical and moral use of cyberspace as an instrument of national power.

The lead Major Command for cyberspace, Air Force Space Command, published a Blueprint for Cyberspace in November 2009 that "provides commander's guidance and intent, identifies opportunities, and delineates objectives and strategies that will shape USAF actions over the next five years, including:

- Creating unique capabilities through innovation and integration
- Building the next-generation network/cyber infrastructure
- Refining operations to create synergies and seamless capabilities
- Fielding and further developing operationally responsive capabilities
- Achieving cyber integration and acculturation[77]

It is clear that the United States and the Air Force are becoming more aggressive in pursuing offensive and defensive cyber capabilities, but there is still a knowledge deficit at the operational level of employment. Colonel Brown is not the only one who suggests that the United States is "much more timid in non-kinetic than kinetic warfare" when authorizing attacks, due primarily to uncertain collateral effects estimates.[78] Colonel Guillermo Carranza, a Staff Judge Advocate at 24th Air Force, also conjectures

[75] Wass de Czege, "Winning in the Cyberelectromagnetic Dimension," 20-32.

[76] Global Security.org, "AN/USQ-163 Falconer Air and Space Operations Center," http://www.globalsecurity.org/military/systems/aircraft/systems/an-usq-163.htm; Northrup Grumman, "Cyber Warfare Integration Center," http://www.as.northropgrumman.com/products/cyberwarfare/index.html (accessed 17 May 2010).

[77] Air Force Space Command, *The United States Blueprint for Cyberspace*, 2 November 2009.

[78] Brown, interview.

that a lack of understanding about the environment and the nature of cyber weapons leads to worst case estimations of possible effects, which contributes to hesitancy in using them to their fullest potential.[79] Improving cyberspace awareness and effects assessment tools and teaching commanders how to use them is imperative for enabling cyber operations—both offensive and defensive.

[79] Colonel Guillermo Carranza (Staff Judge Advocate, 24th Air Force), interview by author, 21 April 2010.

Conclusion

> *The United States will work with like-minded nations to foster norms regarding behavior in domains where an attack on one nation has consequences for all—especially in space and cyberspace.*
>
> -- *2010 Quadrennial Defense Review Report*

It is a platitude that "the United States must create an effective national and international strategic framework for the development and use of cyber as part of an overall national strategy."[1] It is also clear that "denying adversaries of whatever kind the ability to attack our Internet accessible national financial, transportation, power generation, and other information infrastructures in times of war is [a] national priority."[2] Opinions differ; however, on the best implementation of a strategy, or even if a coherent strategy is possible. Many would like to believe that instituting strong domestic laws or ratifying comprehensive international treaties will be enough to solve the problem. On the other hand, Jack Goldsmith and Tim Wu contend that "most people's lives are dominated not by law but by social norms, morality, and the market, [and] the Internet is deeply influenced by its code. But the critical question is whether such sources or rules and governance can function apart from an underlying system of territorial government and physical coercion."[3]

A legitimate and justifiable defense strategy will be grounded in principles of the universally accepted law of armed conflict (LOAC): military necessity, humanity, proportionality, distinction, chivalry, and neutrality. The fundamental purposes of these principles are to:

- Protect both combatants and noncombatants from unnecessary suffering
- Safeguard fundamental human rights
- Facilitate the restoration of peace
- Prevent the deterioration of good order and discipline

[1] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 3.

[2] Huba Wass de Czege, "Winning in the Cyberelectromagnetic Dimension of 'Full Spectrum Operations,'" *Military Review*, March-April 2010, 20-32.

[3] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York, NY: Oxford University Press, 2006), 181.

- Maintain the humanity of soldiers
- Maintain the support of the public[4]

To attain these goals, belligerents must adhere to certain moral and ethical norms of behavior. In cyberspace, these norms can be divided into four general categories: access & connectivity; trust & security; privacy & anonymity; and monitoring & control. It is in the interest of all nation-states to build a framework of international agreements and encourage norms that raise the difficulty of certain types of cyberattacks and perpetuate an environment conducive to the application of LOAC in cyberwarfare.[5]

The decline of the nation-state has been predicted for decades, but it is clear that for the foreseeable future, "the Internet will be shaped by domestic politics and international relations, as interest groups and countries fight for control and influence over the once-borderless medium."[6] Unfortunately, since no international governance exists, it only takes weak domestic law in one state to provide sanctuary for cyber criminals and terrorists. "The Internet's blurring of international lines makes the need for international cooperation that much more critical, if, for no other reason than pure self-preservation, now that any nation can be brought to its knees with the single click of a mouse."[7] Therefore, "the imperative to bring domestic laws in every nation up to a reasonable standard should be readily apparent."[8] However, ambiguities such as the definition of cyber sovereignty, the role of government monitoring and control, and the right to open, anonymous connectivity generate challenging questions, so "as with many novel legal issues, we are likely to discover the answer only from experience."[9]

The moral and ethical ramifications of cyber governance are still being shaped, but in the end, as Robert Gilpin surmises, "governance at any level, whether national or international, must rest on shared beliefs, cultural values, and most of all, a common identity. Unfortunately, we do not yet live in a global civic culture, and few common

[4] International and Operational Law Department, *Operational Law Handbook* (Charlottesville, VA: U.S. Army Judge Advocate General School, 2003), 8.

[5] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND corporation, 2009), 199.

[6] Goldsmith and Wu, *Who Controls the Internet?*, 130.

[7] Daniel M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China," *American University International Law Review 17*, (2002): 641-681.

[8] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, May 1999), 42.

[9] Department of Defense, *Assessment of International Legal Issues in Information Operations*, 19.

values unite all the peoples of the world.... The best for which one can hope is that the major powers, in their own self-interest as well as that of the world in general, will cooperate to fashion a more stable and humane international political and economic order."[10] Cyberspace offers a unique environment for this type of global cooperation, and any solution will require a comprehensive approach using all elements of national power to shape norms of behavior that promote ethical and moral conduct in business, diplomacy, journalism, and warfare.

Military

The military is seemingly the worst instrument of national power to promulgate social norms of behavior in cyberspace. While the individuals associated with the military are normally held in high regard, the public generally does not trust the military to set policy for a nation. This is the reason the United States has a civilian-controlled military. However, the way power is wielded by a society can have a profound influence on the expectations of the populace, and cyber weapons are just another element of power. The law of armed conflict is the codification of universally accepted norms of behavior for warfare, thus it is in the best interest of the international community that norms of behavior in cyberspace reinforce the application of LOAC to cyberwarfare.

While remaining cognizant of the fragility of some cyber *tactics*, the United States would benefit from pulling back the curtain of secrecy hiding *operational* and *strategic* cyber capabilities. It is well known that "although the actual cyberattack capabilities of the United States are highly classified, they are at least as powerful as those demonstrated by the most sophisticated cyberattacks perpetrated by cybercriminals and are likely more powerful."[11] A general misunderstanding of the capabilities and limitations of cyber weaponry hampers effective use of these tools by politicians and military strategists alike. Currently "the lack of explicit generally accepted international norms for cyber conflict reduces the political risk of cyber attack," because there are no

[10] Robert Gilpin, *Global Political Economy* (Princeton, NJ: Princeton University Press, 2001), 402.
[11] National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, eds. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Committee on Offensive Information Warfare, (Washington, DC: The National Academies Press, 2009), 5.

accepted limits to cyberattack, nor are there repercussions for their use.[12] A declaratory statement on what constitutes a legitimate military target in cyberspace may be effective in reassuring our allies and extending deterrence to the newest domain.

An explicit declaration on the limits of cyberattack may also help contain the utilization of such weapons. Throughout history societies have striven to outlaw new instruments of war: crossbows, gunpowder, submarines, and airplanes to name just a few. All efforts have failed. A few weapons however—chemical, biological, and nuclear—have acquired a stigma so strong that their employment is collectively reviled. Generally indiscriminate weapons with the potential to disrupt the fabric of civilization are held in contempt for good reason—they violate all principles of LOAC. Large-scale, capricious proliferation of highly disruptive malware should be discouraged with great prejudice. Any norm of behavior that delegitimizes the use of wide-spread, indiscriminate cyber weapons against critical civilian infrastructure should be supported. Likewise, better understanding of the discriminate nature of more precise cyber weapons is also needed at the unclassified operational and strategic level of command to remove the mystery complicating effective exploitation of cyber weaponry.

Attribution is the key to solving many of the difficulties with limiting cyberattack and applying LOAC to cyberspace. "The Department of Defense continues to improve its ability to attribute WMD, space, and cyberspace attacks in order to hold aggressors responsible and deny them the ability to evade detection in new domains or use proxies."[13] Encouraging the acceptance of monitoring, control, and increased security in the civilian community will enhance the United States' ability to respond to cyberattacks without losing the privacy, access, and connectivity that Americans have come to expect. However, as Colonel Gary Brown states, "Attribution is just a practical problem, not interesting from a doctrine point of view."[14] Whether it is accomplished through

[12] James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies, October 2009, http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (accessed 30 October 2009).

[13] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, February 2010), 14.

[14] Colonel Gary Brown (Staff Judge Advocate, United States Cyber Command), interview by author, 2 November 2009.

technical advancement, procedural controls, or norm de-legitimization, anonymity must be minimized.

Finally, the military needs to reach outside its traditional boundaries to stay ahead of enemies in cyberspace. Cyber security partnerships with communications and manufacturing industries to accelerate the procurement and acquisition process are a start. Another vital task is recruiting talented, innovative personnel, both for frontline operations and research and development. For instance, Peiter Zatko—a respected hacker known as "Mudge"—has been hired as a program manager at the Defense Advanced Research Projects Agency to develop cyber defense tools, and Jeff Moss—aka 'Dark Tangent'—is now a member of the Homeland Security Advisory Council.[15] Using reformed criminals to fight crime is an old tactic, but the military must be careful to maintain the separation of combatants and noncombatants in cyberspace. If civilians or contractors are engaged in cyber combat, they must be designated in some fashion as lawful combatants.

Information/Intelligence

Information and information technology are the blood and bones of cyberspace. Trust relationships based on secure communication form the connective tissue that holds modern society together. The rapidly growing body of scientific and cultural knowledge relies on free, instantaneous retrieval of both objective facts and subjective opinions. Open access to information and the prerogative to utilize information productively breathes life into universal democratic freedoms. David Drummond, Google's chief legal officer has said, "We believe that greater transparency will lead to less censorship. Unless companies, governments and individuals do something, the Internet we know is likely to become ever more restricted—taking choice and control away from users and putting more power in the hands of those who would limit access to information."[16] It is in the interest of the United States to advocate for norms of behavior that uphold the open exchange of information.

[15] Elinor Mills, "Hacker 'Mudge' gets DARPA job," *CNET news*, 10 February 2010, http://news.cnet.com/8301-27080_3-10450552-245.html; "Hacker named to Homeland Security Advisory Council," *CNET news*, 5 June 2009, http://news.cnet.com/8301-1009_3-10258634-83.html?tag=mncol;txt.

[16] Maggie Shiels, "Google Reveals Government Data Requests and Censorship," *BBC News*, 20 April 2010, http://news.bbc.co.uk/2/hi/technology/8633642.stm (accessed 21 April 2010).

In a speech on 21 January 2010 at the Newseum in Washington, DC, Secretary of State Hillary Rodham Clinton professed, "Historically, asymmetrical access to information is one of the leading causes of interstate conflict."[17] Joseph Nye and William Owens also contend that control over information will be the ultimate source of power in the international politics of the Internet age.[18] The battle over information begins with accurate, timely, and specific intelligence about an adversary's capabilities and intentions. Detailed intelligence regarding networks and information systems is critical to the success of cyberattack, so it is in the interest of all nations to protect this knowledge. However, in order to support LOAC, it is also necessary to distinguish between combatant and noncombatant equipment, personnel, and actions. This necessitates either extensive intelligence work to minimize collateral damage, or delineation and designation of legitimate targets through treaties and declaratory statements.

Reining in non-state actors also requires extensive, time-sensitive intelligence. International cooperation is needed to delegitimize anonymity in order to ferret out cyber criminals, but this must be balanced with reasonable concerns about the right to privacy. Trust in government to do the right thing in the United States is at an all time low, but online "government data users tend to have more positive attitudes towards government openness and accountability."[19] Promoting trust in government online will help alleviate fears of monitoring and enhance cyberspace security. Engendering this trust in other societies, or in a global system of governance, will entail a great deal of diplomacy.

Diplomacy

In her speech on Internet freedom, Secretary Clinton launched a major new initiative to foster open access to the Internet. She added the 'freedom to connect' to Franklin Delano Roosevelt's four fundamental freedoms: freedom of expression, freedom

[17] Hillary Rodham Clinton, "Remarks on Internet Freedom," (speech, Newseum, Washington, DC, 21 January 2010). http://www.state.gov/secretary/rm/2010/01/135519.htm

[18] Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* 75, 2 (March/April 1996): 20-36 quoted in Robert Gilpin, *Global Political Economy*, (Princeton, NJ: Princeton University Press, 2001), 394.

[19] Pew Research Center, "Distrust, Discontent, Anger and Partisan Rancor," 18 April 2010, http://people-press.org/report/606/trust-in-government (accessed 6 May 2010); Aaron Smith, "Government Online" (Washington, DC: Pew Internet & American Life Project, April 2010), 5.

of worship, freedom from want, and freedom from fear.[20] She also encouraged countries around the world to support "a single Internet where all of humanity has equal access to knowledge and ideas."[21] This would involve significant changes in many nations' law and policy, including the United States; however, this endeavor supports the norms of trust, access, and connectivity.

Kristen Lord is correct when she states, "Wars, ever more, are wars of ideas and credibility as well as wars of might."[22] While cyber power has yet to demonstrate the ability to rival J. C. Wylie's "gun on the ground" as a coercive tool, it has a demonstrable effect on international security relations through the propagation of, and access to, information.[23] The United States should foster global cooperation by engaging nation-states—specifically China and Russia—to join in a propaganda war against malfeasant non-state actors while discouraging state-sponsored cyberattacks. The United States should also be careful to "match statements, actions, and policies" to maintain global credibility.[24] A statement making no distinction between those who commit cyberattacks and those who support and harbor them would put tangible power behind a deterrent cyber policy and reverse the norm of anonymity protecting plausibly deniable state-sponsored cyberattacks. [25]

According to the State Department, "the government is regularly engaged in in-depth conversations with tech companies about how their technologies are being used to foster human rights and how those companies can help promote Internet access and

[20] The "four essential human freedoms" were first proclaimed by President Franklin Delano Roosevelt in the 6 January 1941 State of the Union Address. He also set down the guidelines for the Lend-Lease Act and proposed what would end up being Social Security, Medicare, and Welfare. Finally, he listed some basic expectations of our political and economic systems: equality of opportunity for youth and for others; jobs for those who can work; security for those who need it; the ending of special privilege for the few; the preservation of civil liberties for all; and the enjoyment of the fruits of scientific progress in a wider and constantly rising standard of living. A transcript and audio file of this foundational speech can be found at http://www.americanrhetoric.com/speeches/fdrthefourfreedoms.htm.

[21] Clinton, "Remarks on Internet Freedom."

[22] Kristen M. Lord, *The Perils and Promise of Global Transparency* (Albany, NY: State University of New York Press, 2006), 4.

[23] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1967), 2.

[24] Lord, *Perils and Promise of Global Transparency*, 129.

[25] This is an obvious adaptation to the famous statement, "We will make no distinction between those who commit acts of terror and those who support and harbor them." George W. Bush, *The National Security Strategy of the United States of America* (Washington DC: United States Government, 2006), 12.

freedom."[26] This is a change from Defense Department guidance in 1999: "There seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations."[27] Obviously the increase in cyber crime and espionage over the past decade has affected this decision, and the potential for cyberwarfare in the future has intensified the need for global engagement. In order to strengthen global cyber defense, the United States must accept responsibility for the role it plays in propagating cyber weaponry and be willing to implement stronger domestic and international laws against cyber criminals.

Legal

Diplomatic efforts will also be needed to close the gaps between international law enforcement, nongovernmental security, and national military preparations. Due to its transnational nature and ease of access, cyberspace is more like the global commons of the environment than a strategic asset. International agreements such as the Council of Europe's Convention on Cybercrime are a solid step in the right direction towards peaceful cooperation on cyber governance, yet they "suffer from a lack of wide acceptance, adequate enforcement and an inability to conclusively identify the source of cyber attacks and intrusions."[28] Comprehensive multilateral treaties enhancing cooperation against cybercrime, stricter international laws proscribing the proliferation of malware, and unilateral declaratory statements foreswearing the first or widespread persistent use of cyberattacks against non-military targets will promote the norms of trust and security and delegitimize anonymity.

The anonymity achievable in cyberspace is unparalleled in any other domain. This complicates attribution, neuters deterrence, incites criminal impunity, and generally encourages bad norms of behavior. Most of the literature concerning cyber security is paralyzed by the puzzle of attribution. Why do people expect anonymity in cyberspace?

[26] J. Nicholas Hoover, "Clinton Calls on Businesses to Support Internet Freedom," *Information Week*, 21 January 2010, (accessed 16 February 2010), http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222400095.

[27] Department of Defense, *Assessment of International Legal Issues in Information Operations*, 50.

[28] Abraham M. Denmark et al. eds., *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security Report, January 2010, (accessed 12 February 2010), 150. http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

Perhaps it is because they can, through anonymizing services such as I2P and TOR, attain a level of anonymity that is nearly impossible in the real world. Proponents argue that it is impossible to do away with anonymity without losing privacy. However, users in every other domain are required to register vehicles—cars, boats, planes, even spacecraft—for ease of identification, and in most cases operators require a license. If a user was required to register their computer or IP address with an internet service provider or obtain a public key license to access the Internet, as an automobile driver is required to do for access to the transit system, the problem of attribution could be resolved without infringing on privacy. Stronger domestic regulation and international coordination are the only way to influence the norm of anonymity in cyberspace, and removing anonymity is the only way to fully implement LOAC in cyberwarfare. The international community has typically shown support for the norms of privacy and security—two universal human rights—but finding a balance between monitoring and control is more complicated.

Infrastructure

Collaborative research and development is also needed into methods for improved attribution, precise retribution, and a more secure Internet architecture. The United States and other responsible state and non-state actors should do everything in their power to hasten the transformation of internet protocol infrastructure to IPv6 or a more modern, secure design. This is not only necessary for continued growth of the Internet, since the current address space of IPv4 is nearly exhausted, but it can also strengthen cyber defenses by eliminating the need for network address translation and IP masquerading, thus removing a source of anonymity. However, there are other security implications due to the large available address space and inevitable bugs of implementing a new system.[29] Other improvements include designing cyber weapons that are more discriminatory and improving cyber assessment tools to mollify commanders who are currently unwilling to use them due to collateral damage risks. Also, declassifying offensive weapons at the operational and strategic level will give commanders a better understanding of their capabilities and limitations, and facilitate their integration into exercise and real-world

[29] For a brief description of this transition from IPv4 to IPv6 see Edward Skoudis, “Evolutionary Trends in Cyberspace,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 155-156.

plans. Finally, tighter collaboration between law enforcement, military, and information technology security industries will close the gaps that currently exist in our cyber defenses. These steps should help address national security challenges by building a “comprehensive framework to ensure a coordinated response by Federal, state, local … and international allies to significant incidents” as outlined in President Obama’s Cyber Policy Review.[30] United States Cyber Command is the obvious administrative agent to manage and control these tasks, but the majority of work will be accomplished in the commercial sector.

Economy

Much of social and technological progress—and political strife—can be explained by the pursuit of economic goals. Man’s desire to live comfortably, and secure the resources to do so, have led to norms of behavior that alternately encourage the collectivization or accretion of wealth. Cyberspace has not varied this trend, it has amplified it. “By coordinating individual Internet users on a large-scale basis, consumer advocates have been able to circumvent many established legal institutions in favor of a more bottom-up type of activism.... ‘peer pressure with a stick’ has thus emerged as another type of Internet norm.”[31] Business models and economic trends are strong motivators for social change and powerful drivers of norms of behavior; they should be exploited to enable the use of LOAC in cyberwarfare.

The economic approach is also supported by “General Chilton of the Strategic Command and Gen. James E. Cartwright, the vice chairman of the Joint Chiefs of Staff, [who] have been urging the United States to think more broadly about ways to deter attacks by threatening a country’s economic well-being or its reputation.”[32] This is a reflection of the international, interagency approach necessary to control cyberspace, because we cannot rely on unilateral action or a lone element of national power. Robert

[30] White House, *Cyberspace Policy Review*, May 2009, (accessed 17 December 2009), v. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[31] Marcelo Halpern and Ajay K. Mehrota, “From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age,” *University of Pennsylvania Journal of International Economic Law 21*, (Fall 2007): 523-561.

[32] John Markoff, David E. Sanger, and Thom Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent,” *The New York Times*, 25 January 2010, (accessed 1 April 2010) http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=1&partner=rss&emc=rss

Gilpin opines, “Although a liberal international economic order does reflect the interests of a dominant power, such a power cannot impose a liberal economic order on the rest of the world; ultimately, the regime must rest on international cooperation.”[33] Policymakers concur, “Enduring unilateral dominance in cyberspace is neither realistic nor achievable by the United States,” but we *do* have considerable influence on international norms of behavior.[34] It is in the United States’ national interest to advance norms that will ensure moral and ethical conduct of cyberwarfare, including international cooperation to promote open access to information, assured freedom of expression, security standardization, and attributable connectivity in cyberspace.

[33] Gilpin, *Global Political Economy*, 88.

[34] National Research Council, *Technology, Policy, Law, and Ethics*, 5.

Bibliography

Academic Papers

Jamison, Marc. “Sanctuaries: A Strategic Reality, an Operational Challenge.” Strategy Research Project. US Army War College, 2008.

Lewis, James A. *The “Korean” Cyber Attacks and Their Implications for Cyber Conflict*. Center for Strategic and International Studies, October 2009. http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (accessed 30 October 2009).

Rogers, John C. *Shaping the Air Force Operational Environment in Cyberspace*. Air War College research report. Maxwell AFB, AL: Air University, 12 February 2009.

Sofaer, Abraham D., and Seymour E. Goodman. *A Proposal for an International Convention on Cyber Crime and Terrorism*. Stanford, CA: The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP), and The Center for International Security and Cooperation (CISAC), August 2000. http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (accessed 1 April 2010).

Articles (News)

Acohido, Byron. “Some Russian PCs Used to Cyberattack Georgia.” *USA Today*, 17 August 2008. http://www.usatoday.com/tech/news/computersecurity/hacking/2008-08-17-russia-georgia-war-hackers_N.htm (accessed 5 May 2010).

Baker, Stephen. “Taming of the Internet.” *Business Week*, 15 December 2003. http://www.businessweek.com/magazine/content/03_50/b3862091_mz063.htm. (accessed 16 February 2010).

Goldmith, Jack. “Can We Stop the Cyber Arms Race?” *Washington Post*, 1 February 2010.

Gray, Andrew. “Georgia Hacking Stirs Fears of Cyber Militias.” *Reuters*, 1 September 2008. http://www.reuters.com/article/idUSN2945446120080901 (accessed 15 February 2010).

Hoover, J. Nicholas. “Clinton Calls on Businesses to Support Internet Freedom.” *Information Week*, 21 January 2010. http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222400095 (accessed 16 February 2010).

Hughes, Rex B. “NATO and Cyber Defence.” *Atlantisch Perspectief 8*, 2008 http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (accessed 19 March 2010).

LaFraniere, Sharon, and Jonathan Ansfield. “China Alarmed by Security Threat from Internet,” *New York Times*, 11 February 2010. http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html (accessed 16 February 2010).

Leyne, Jon. “How Iran’s Political Battle is Fought in Cyberspace.” *BBC News*, 11 February 2010. http://news.bbc.co.uk/2/hi/8505645.stm (accessed 15 March 2010).

Liu, Henry C. K. "China—The Abduction of Modernity—Part 3: Rule of Law vs. Confucianism." *Asia Times*, 24 July 2003. http://www.atimes.com/atimes/China/EG24Ad01.html (accessed 22 March 2010).

Luard, Tim. "Chinese Activists Evade Web Controls." *BBC online*, 30 January 2004. http://news.bbc.co.uk/2/hi/asia-pacific/3440911.stm (accessed 17 May 2010).

Markoff, John, and Thom Shankar. "Halted '03 Iraq Plan Illustrates US Fear of Cyberwar Risk." *New York Times*, 1 August 2009. http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=1 (accessed 1 April 2010).

Markoff, John, and Andrew Kramer. "In Shift, U.S. Talks to Russia on Internet Security." *New York Times*, 12 December 2009. http://www.nytimes.com/2009/12/13/science/13cyber.html (accessed 10 February 2010).

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times*, 25 January 2010. http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=1&partner=rss&emc=rss (accessed 1 April 2010).

Matyszczyk, Chris. "Google Gets Buzzed With Class Action Lawsuit." *CNET News*, 17 February 2010. http://news.cnet.com/8301-17852_3-10455573-71.html (accessed 24 February 2010).

McMillan, Robert. "Spanish Police Take Down Massive Mariposa Botnet." *Networkworld*, 2 March 2010. http://www.networkworld.com/news/2010/030310-spanish-police-take-down-massive.html (accessed 24 March 2010).

Mills, Elinor. "Hacker 'Mudge' gets DARPA job." *CNET news*, 10 February 2010. http://news.cnet.com/8301-27080_3-10450552-245.html (accessed 16 February 2010).

Mills, Elinor. "Hacker named to Homeland Security Advisory Council." *CNET news*, 5 June 2009. http://news.cnet.com/8301-1009_3-10258634-83.html?tag=mncol;txt (accessed 16 February 2010).

Morozov, Evgeny. "Is Russia Google's Next Weak Spot?" *Foreign Policy: Net Effect*, 26 March 2010. http://neteffect.foreignpolicy.com/blog/5386 (accessed 30 March 2010).

Schogol, Jeff. "Official: No Options 'Off the Table' for U.S. Response to Cyber Attacks." *Stars and Stripes*, 8 May 2009. http://www.stripes.com/article.asp?section=104&article=62555 (accessed 26 March 2010).

Shacthman, Noah. "Air Force Suspends Controversial Cyber Command." *Danger Room, Wired.com*, 13 August 2008. http://www.wired.com/dangerroom/2008/08/air-force-suspe/ (accessed 29 March 2010).

Shalal-Esa, Andrea. "US Military Sees Rising Demand for Satellites." *Reuters*, 2 June 2008. http://www.reuters.com/article/idUSN0229389520080602 (accessed 1 April 2010).

Tedford, Deborah. "Goggle to Shift Chinese Users to Hong Kong." *NPR*, 22 March 2010. http://www.npr.org/templates/story/story.php?storyId=125028043&sc=emaf (accessed 22 March 2010).

Wakefield, Jane. "Google Bosses Convicted in Italy." *BBC News*, 24 February 2010. http://news.bbc.co.uk/2/hi/technology/8533695.stm (accessed 24 February 2010).

Whitney, Lance. “With Legal Nod, Microsoft ambushes Waledac Botnet.” *CNET news*, 25 February 2010. http://news.cnet.com/8301-1009_3-10459558-83.html (accessed 24 March 2010).

Wolf, Jim. “Google Puts Focus on China Cyberwar Fears.” *Reuters*, 20 January 2010. http://www.reuters.com/article/idUSTRE60J5PK20100120 (accessed 21 January 2010).

Articles (Journal)

Brown, Davis. “A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict.” *Harvard International Law Journal 47 no. 1*, (Winter 2006): 179-221.

Condron, Sean M. “Getting it Right: Protecting American Critical Infrastructure in Cyberspace.” *Harvard Journal of Law and Technology 20*, (Spring 2007): 404-422.

Creekman, Daniel M. “A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China.” *American University International Law Review 17*, (2002): 641-681.

Czege, Huba Wass de. “Winning in the Cyberelectromagnetic Dimension of ‘Full Spectrum Operations.’” *Military Review*, March-April 2010, 20-32.

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.”*International Organization* 52, no. 4 (1998): 887-917.

Fischer-Lescano, Andreas, and Gunther Teubner. “Reply to Andreas L. Paulus Consensus as Fiction of Global Law.” *Michigan Journal of International Law 25*, (Summer 2004): 1059-1073.

Grant, Rebecca. “The Cyber Menace.” *Airforce-Magazine.com 92, no. 3*. (March 2009). http://www.airforce-magazine.com/MagazineArchive/Pages/2009/March%202009/0309cyber.aspx

Gutmann, Ethan. “Hacker Nation: China’s Cyber Assault.” *World Affairs Journal*, (May/June 2010). http://www.worldaffairsjournal.org/articles/2010-MayJune/full-Gutmann-MJ-2010.html.

Halpern, Marcelo, and Ajay K. Mehrota. “From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age.” *University of Pennsylvania Journal of International Economic Law 21*, (Fall 2007): 523-561.

Jurich, Jon P. “Cyberwar and Customary International Law.” *Chicago Journal of International Law 9*, no. 1 (Summer 2008): 275-294.

Lewis, Jonathan Eric. “The Economic Espionage Act and the Threat of Chinese Espionage in the United States.” *Chicago-Kent Journal of Intellectual Property* 8, no. 2 (Spring 2009): 189-236.

McGavran, Wolfgang. “Intended Consequences: Regulating Cyber Attacks.” *Tulane Journal of Technology and Intellectual Property 12*, (Fall 2009): 259-275.

Paulus, Andreas L. “Commentary to Andreas Fischer-Lescano & Gunther Teubner: The Legitimacy of International Law and the Role of the State.” *Michigan Journal of International Law 25*, (Summer 2004): 1047-1058.

Perry, Chondra. “Social Media and the Army.” *Military Review*, March-April 2010, 20-32.

Rittel, Horst W. J., and Melvin M. Webber.“Dilemmas in a General Theory of Planning.” *Policy Sciences 4*, (1973): 155-169.

Schmitt, Michael N. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” *The Columbia Journal of Transnational Law 37* (1999): 885-937.

Shackelford, Scott J. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.” *Berkeley Journal of International Law 27*, (2009): 192-251.

Shulman, Mark. “Discrimination in the Laws of Information Warfare.” *Columbia Journal of Transnational Law 37 (Notes)*, (1999): 939-968.

Sonbuchner, Scott P. “Master Your Domain: Should the U.S. Government Maintain Control over the Internet’s Root?” *Minnesota Journal of International Law 17,* (Winter 2008): 183-207.

Terry, James P. “The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Conflict: What are the Targeting Constraints?” *Military Law Review 169*, (September 2001): 70-89.

Walker, George K. “Information Warfare and Neutrality.” *Vanderbilt Journal of Transnational Law* 33(5), (November 2000):1079-1200.

Wimmer, Kurt. “International Processes: Toward a World Rule of Law: Freedom of Expression.” *The Annals of The American Academy of Political and Social Science 603*, (January 2006): 202-216.

Books

Brandt, R. B. “Utilitarianism and the Rules of War.” In *War and Moral Responsibility*, edited by Marshall Cohen, Thomas Nagel, and Thomas Scanlon. Princeton, NJ: Princeton University Press, 1974.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York, NY: Oxford University Press, 2009.

Brownlie, Ian. *Principles of Public International Law*. 7th ed. Oxford, England: Oxford University Press, 2008.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Corbett, Julian S. *Some Principles of Maritime Strategy*. London, England: Longmans, Green & Co., 1911.

Finnemore, Martha. *National Interests in International Society*. Ithaca, NY: Cornell University Press, 1996.

Fuerth, Leon. “Cyberpower from the Presidential Perspective.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Garner, Bryan A. et al., ed. *Black’s Law Dictionary*. 7th ed. St. Paul, MN: West Group, 1990.

Gilpin, Robert. *Global Political Economy*. Princeton, NJ: Princeton University Press, 2001.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?* New York, NY: Oxford University Press, 2006.

Grayling, A.C. *Among the Dead Cities*. New York, NY: Walker & Company, 2006.

Holmes, Richard et al., ed. *The Oxford Companion to Military History*. Oxford, England: Oxford University Press, 2001.

Howard, Michael. “Constraints on Warfare.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Kagan, Robert. *Of Paradise and Power: America and Europe in the New World Order*. New York, NY: Vintage, 2004.

Katzenstein, Peter, ed. *The Culture of National Security: Norms and Identity in World Politics*. New York, NY: Columbia University Press, 1996.

Kennedy, Paul, and George J. Andreopoulos. “The Laws of War: Some Concluding Reflections.” In *The Laws of War: Constraints on Warfare in the Western World,* edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Keohane, Robert. *After Hegemony*. Princeton, NJ: Princeton University Press, 1984.

Kramer, Franklin D. “Cyberpower and National Security: Policy Recommendations for a Strategic Framework.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Kuehl, Daniel T. “From Cyberspace to Cyberpower: Defining the Problem.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Kwalwasser, Harold. “Internet Governance.” In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Libicki, Martin. *Conquest in Cyberspace*. New York, NY: Cambridge University Press, 2007.

Libicki, Martin. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Lord, Kristen M. *The Perils and Promise of Global Transparency*. Albany, NY: State University of New York Press, 2006.

Machiavelli, Nicolo. *The Prince*. Translated by W. K. Marriott. Rockville, MD: Arc Manor, 2007.

Nagel, Thomas. “War and Massacre.” In *War and Moral Responsibility,* edited by Marshall Cohen, Thomas Nagel, and Thomas Scanlon. Princeton, NJ: Princeton University Press, 1974.

National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin. Committee on Offensive Information Warfare, Washington, DC: The National Academies Press, 2009.

Neff, Stephen C. *War and the Law of Nations*. Cambridge, England: Cambridge University Press, 2005.

Nelson, Richard Alan. *A Chronology and Glossary of Propaganda in the United States*. Westport, CT: Greenwood Press, 1996.

Nye Joseph S., Jr., and William A. Owens. “America’s Information Edge.” *Foreign Affairs* 75, 2 (March/April 1996): 20-36 quoted in Robert Gilpin, *Global Political Economy*. Princeton, NJ: Princeton University Press, 2001.

Nye, Joseph S., Jr. *Soft Power: the Means to Success in World Politics*. New York, NY: Public Affairs, 2004.

Ober, Josiah. “Classical Greek Times.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Pape, Robert A. *Bombing to Win*. Ithaca, NY: Cornell University Press, 1996.

Parker, Geoffrey. “Early Modern Europe.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Reisman, W. Michael, and Chris T. Antoniou, eds. *The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict*. New York, NY: Vintage Books, 1994.

Roberts, Adam. “Land Warfare: From Hague to Nuremberg.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Rothenberg, Gunther. “The Age of Napoleon.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Sewell, Sarah. *Introduction to the U.S. Army and Marine Corps Counterinsurgency Field Manual*. Chicago, IL: The University of Chicago Press, 2007.

Stacey, Robert C. “Age of Chivalry.” In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos, and Mark R. Shulman. New Haven, CT: Yale University Press, 1994.

Strassler, Robert B. *The Landmark Thucydides*. New York, NY: Simon & Schuster, 1996.

Tzu, Lao. *Tao Te Ching*. Edited and translated by Jonathan Star. New York, NY: Penguin, 2001.

Tzu, Sun. *The Illustrated Art of War*. Edited and translated by Samuel B. Griffith. Oxford, England: Oxford University Press, 2005.

Waltz, Kenneth. *Theory of International Politics*. Boston, MA: McGraw Hill, 1979.

Walzer, Michael. *Just and Unjust Wars*. 4th ed. New York, NY: Basic Books, 2006.

Walzer, Michael. “Political Action: The Problem of Dirty Hands.” In *War and Moral Responsibility*, edited by Marshall Cohen, Thomas Nagel, and Thomas Scanlon. Princeton, NJ: Princeton University Press, 1974.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge, UK: Cambridge University Press, 1999.

Wilson, Clay. “Cyber Crime.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Wylie, J. C. *Military Strategy: A General Theory of Power Control*. Annapolis, MD: Naval Institute Press, 1967.

Briefings/Point Papers/Memos/Messages

Ivanov, Igor, Minister for Foreign Affairs of the Russian Federation. To Kofi Annan, United Nations Secretary-General. Letter, 20 September 1998.

Jefferson, Thomas. To John Jay. Letter, 1786 quoted in University of Virginia, *Jeffersonian Cyclopedia*, ed. John Foley (New York, NY: Funk & Wagnalls, 1900), no. 4702. Found in Jefferson Digital Archive http://etext.virginia.edu/etcbin/foley-page?id=JCE4702 (accessed 22 February 2010).

Luck, Gary, and Mike Findlay. *Joint Operations Insights and Best Practices*. 2nd ed. Suffolk, VA: USJFCOM Joint Warfighting Center, July 2008.

United States Department of Commerce. *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule.* US Government Green Paper. National Telecommunications and Information Administration. Washington, DC: Federal Register, 20 February 1998. 15 CFR Chap. XXIIII, Vol. 63, No. 34, pg. 8827. http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.txt.

Government Documents

Air Force Doctrine Document (AFDD) 2-11. *Cyberspace Operations*. (draft).

Air Force Doctrine Document (AFDD) 3-12. *Cyberspace Operations*. (draft).

Air Force Public Affairs Agency. *Social Media and the Air Force* version 2. Arlington, VA: Emerging Technology Division, November 2009.

Air Force Space Command. *The United States Blueprint for Cyberspace*, 2 November 2009.

Bush, George W. *The National Security Strategy of the United States of America*. Washington DC: United States Government, 2006.

Charter of the United Nations. San Fransisco, CA, 24 October 1945.

Council of Europe. *Convention on Cybercrime.* Budapest, Hungary: European Treaty Series No. 185, 23 November 2001.

Geneva Conference. *Convention for the Amelioration of the Condition of the Wounded in Armies in the Field*. 22 August 1864.

Geneva Conference. *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 12 August 1949.

Geneva Conference. *Convention (IV) Relative to the Protection of Civilian Persons in Time of War*. 12 August 1949.

Geneva Conference. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* 8 June 1977.

Geneva Conference. *Convention on Prohibitions of Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*. 10 October 1980.

Hague Conference. *Convention with Respect to the Laws and Customs of War on Land (Hague II)*. 29 July 1899.

Hague Conference. *Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V)*. 18 October 1907.

House. *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Testimony before the Committee on Foreign Affairs*. 10 March 2010.

International and Operational Law Department. *Operational Law Handbook*. Charlottesville, VA: U.S. Army Judge Advocate General School, 2003.

Joint Publication 3-13. *Information Operations*, 13 February 2006.

Judge Advocate General School. *The Military Commander and the Law*. 8th ed. Maxwell Air Force Base, AL: U.S. Air Force Judge Advocate General's School, 2006.

Presidential Decision Directive NSC-63. Critical Infrastructure Protection, 22 May 1998.

Saint Petersburg Conference. *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*. 11 December 1868.

United Nations General Assembly. *The Universal Declaration of Human Rights*. 10 December 1948. http://www.un.org/en/documents/udhr/index.shtml.

US Department of Defense. *Quadrennial Defense Review Report*. Washington, DC: Government Printing Office, February 2010.

US Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC: Government Printing Office, 2009.

White House. *Cyberspace Policy Review*. May 2009, (accessed 17 December 2009). http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Personal Communications

Brown, Colonel Gary, Staff Judge Advocate, United States Cyber Command. Interview by author, 2 November 2009.

Carranza, Colonel Guillermo, Staff Judge Advocate, 24th Air Force. Interview by author, 21 April 2010.

Reports

Denmark, Abraham M. et al., eds. *Contested Commons: The Future of American Power in a Multipolar World*. Center for a New American Security Report. January 2010. http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf (accessed 12 February 2010).

Department of Defense. *An Assessment of International Legal Issues in Information Operations*. Washington, DC: Office of General Counsel, May 1999.

Frankel, Sheila, Richard Graveman, and John Pearce. *Guidelines for the Secure Deployment of IPv6 (draft)*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Division, February 2010, Special Publication 800-119.

Kurtz, Paul B. “Virtual Criminology Report 2009.” Santa Clara, CA: McAfee, Good Harbor Consulting, 2009.

Mesic, Richard, et al. “Air Force Cyber Command (Provisional) Decision Support.” RAND report, Santa Monica, CA, 2010.

Moteff, John. *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*. Congressional Research Service Report. Washington, DC: Library of Congress, 16 April 2004.

Pew Research Center. “Distrust, Discontent, Anger and Partisan Rancor.” 18 April 2010. http://people-press.org/report/606/trust-in-government (accessed 6 May 2010).

Rosenzweig, Paul. “National Security Threats in Cyberspace.” Workshop report. American Bar Association Standing Committee on Law and National Security, Annapolis, MD, 4-5 June 2009.

Smith, Aaron. “Government Online.” Washington, DC: Pew Internet & American Life Project, April 2010.

United Nations General Assembly. Report of the Secretary-General on the Work of the Organization. *An Agenda for Peace: Preventive Diplomacy, Peacemaking and Peacekeeping*. U.N. Doc. A/47/277/S/2411, 17 June 1992.

United Nations General Assembly. Report of the Secretary-General on the Work of the Organization. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* U.N. Doc. A/60/202, 5 August 2005, (accessed 17 December 2009). http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

Speeches/Statements

Chilton, Kevin P., Commander United States Strategic Command, Speech. 2009 Cyberspace Symposium, Omaha, NE, 7 April 2009, (accessed 23 March 2010). http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium

Clinton, Hillary Rodham, United States Secretary of State. "Remarks on Internet Freedom." Speech. Newseum, Washington, DC, 21 January 2010. http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed 22 January 2010).

Dunlap, Major General Charles J., Jr., Former Deputy Staff Judge Advocate General of Air Force. "Towards a Cyberspace Legal Regime in the Twenty-First Century." Speech. Air University Cyberspace Symposium, Maxwell AFB, AL, 16 July 2008.

Sommaruga, Cornelio, President of the ICRC. *Appeal by the International Committee of the Red Cross on the 20th anniversary of the adoption of the Additional Protocols of 1977*. Statement. 31 October 1997, http://www.icrc.org/web/eng/siteeng0.nsf/html/57JNUX (accessed 23 March 2010).

Websites

Alexa, the Web Information Company. http://www.alexa.com/

American Registry for Internet Numbers. https://www.arin.net/.

Computer Emergency Response Team. "LEVANT." http://www.cert.org/sse/levant.html.

Cooperative Cyber Defence Centre of Excellence. http://www.ccdcoe.org/.

Counter for remaining IP address. http://www.inetcore.com/project/ipv4ec/index_en.html

Electronic Frontier Foundation. http://www.eff.org/.

Geneva Conventions and Protocols. http://www.icrc.org/ihl.nsf/CONVPRES?OpenView.

Global Internet Freedom Consortium. http://www.internetfreedom.org/

Global Network Initiative. http://www.globalnetworkinitiative.org/.

Information Security Forum. https://www.isfsecuritystandard.com/SOGP07/index.htm

International Telecommunications Union. http://www.itu.int/en/pages/default.aspx.

Internet Assigned Numbers Authority. http://www.iana.org/.

Internet Corporation for Assigned Names and Numbers. http://www.icann.org/.

Internet Engineering Task Force. http://www.ietf.org/.

Partnership for Peace Information Management System. http://www.pims.org/.

Privacy International. http://www.privacyinternational.org/.

Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/

The Committee on National Security Systems. http://www.cnss.gov/index.html.

Wikileaks. https://secure.wikileaks.org/.

Appendix A

Computer Fraud and Abuse Act

Computer crime in the United States was initially limited in 1986 with the codification of 18 U.S.C. § 1030, one of the primary instruments in the fight against cyber crime. This legislation can be used to prosecute anyone who obtains unauthorized access, transmits data, or damages protected computers with the intent to defraud, extort, or injure individuals, agencies of the government, or financial institutions in the United States.[1] The law has been amended numerous times, the latest of which was the Identity Theft and Enforcement and Restitution Act in 2008.

Communications Assistance for Law Enforcement Act

This act, codified in 1994 in 47 U.S.C. §§ 1001-10, requires telecommunications carriers and manufacturers to design equipment with built-in surveillance capabilities to allow federal agencies to monitor all traffic in real-time when authorized by law. As stated on their website, "The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness."[2] The most significant development with this law has been its implementation in accordance with the Patriot Act of 2001 to authorize warrantless wiretapping.

Information Technology Management Reform Act

This legislation, 40 U.S.C. §§ 1401 passed in 1996, regulates the acquisition of information technology to ensure efficiency, security, and privacy of federal computer systems. It also established a process, through the National Institute of Standards and Technology, to develop standards for secure interoperability and portability of data and software. Most significantly, it defines information technology as "any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching,

[1] U.S. Code Title 18 Part I Chapter 47 Sec 1030, found at: Cornell University Law School, http://www.law.cornell.edu/uscode/18/1030.html (accessed 24 March 2010).

[2] Ask CALEA, 27 August 2009, http://www.askcalea.net/ (accessed 24 March 2010).

interchange, transmission, or reception of data or information by the executive agency."[3] This definition has since been used repeatedly throughout the United States government to delimit information technology and cyberspace.

Economic Espionage Act

The United States government made a noteworthy attempt to curb cyber espionage with the Economic Espionage Act in 1996 (18 U.S.C. §§ 1831-9). This legislation "does not require that prosecutors prove that a foreign government or entity needed to be involved, directly or indirectly, in the theft of trade secrets. Rather, what is required is for a person or organization to act in such a way that will benefit a foreign government or entity."[4] This legislation is important, because it outlines what the United States considers to be economic espionage, but it does nothing to define what constitutes an act of cyberwar.

Federal Information Security Management Act

The FISMA, part of the E-Government act of 2002 (44 U.S.C. §§ 3541-9), is the widest reaching legislation concerning federal requirements to establish cyber security programs. Essentially it "requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."[5] There has been a long-standing debate on how much the government should extend this requirement to private industry.

[3] This definition has since been used extensively in throughout U.S. government doctrine. Division E—Information Technology Management Reform, Sec. 5002(3), http://govinfo.library.unt.edu/npr/library/misc/s1124.html (accessed 24 March 2010).

[4] Jonathan Eric Lewis, "The Economic Espionage Act and the Threat of Chinese Espionage in the United States," *Chicago-Kent Journal of Intellectual Property* 8, no. 2 (Spring 2009): 189-236.

[5] National Institute for Standards and Technology, "FISMA Detailed Overview," Computer Security Division, 9 March 2010, http://csrc.nist.gov/groups/SMA/fisma/overview.html (accessed 24 March 2010).

Appendix B

Draft Convention Regulating the Use of Information Systems in Armed Conflict[6]

The High Contracting Parties,
[preambular paragraphs]
have agreed to the following:

I. General

Article 1

a. The term “information attack” means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial-of-service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target, for the purpose of inflicting injury or degrading the enemy’s ability or will to fight.

b. The term “use of information systems in armed conflict” means the use of computers and/or other information and communications systems in an information attack, as opposed to use for the sole purpose of communication, intelligence gathering, logistical support, passive computer network defense, or other force enhancements.

c. The term “State” includes all organs and instrumentalities of any administration purporting to govern the territory and population of an area, whether or not that area is recognized as a State, and whether or not the government is recognized as legitimate.

d. The term “law of armed conflict” means the body of law that regulates the conduct of persons in armed conflict, and encompasses the terms “international humanitarian law,” “law of war,” and “*jus in bello*.”

Article 2

This Convention regulates the use of information systems in armed conflict, applying and upholding the generally accepted principles of distinction, military necessity, humanity, proportionality, and chivalry.

Article 3

An act that violates the law of armed conflict if carried out by conventional means also violates the law of armed conflict if carried out by an information attack. An attack that does not violate the law of armed conflict if carried out by conventional means also does not violate the law of armed conflict if carried out using information systems. A common crime that is committed using information systems, such as larceny, violates the law of

[6] Copied in full from Davis Brown, “A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict,” *Harvard International Law Journal 47 no. 1*, (Winter 2006): 179-221.

armed conflict if it is committed by lawful or unlawful combatants in furtherance of an armed conflict.

II. Distinction

Article 4

The term “combatant” shall designate any member of the regular, uniformed armed services of a State, including reserves and national guard, and uniformed internal security and law enforcement services as Parties shall designate; and other armed forces and organized resistance movements meeting all of the following conditions:

a. they are commanded by a person responsible for his or her subordinates;

b. they wear uniforms or other fixed distinctive signs recognizable at a distance;

c. they carry their arms openly; and

d. they conduct their operations in accordance with the laws and customs of war.

The term “combatant” shall not include medical or religious personnel.

Article 5

The term “noncombatant” shall designate any person who is not a combatant as defined in Article 4 above.

Article 6

For the purpose of this Convention, civilians engaged in a *levée en masse* shall not be considered lawful combatants.

Article 7

Only lawful combatants shall be permitted to engage in information attacks on other States. This Convention shall not restrict the capacity of noncombatants to use information systems for communications, logistical support, or other force enhancement systems, provided such uses do not otherwise violate the prohibitions set forth in this Convention or the principles of the law of armed conflict.

Article 8

States shall engage in information attacks in only facilities located a safe distance away from facilities used by noncombatants.

Article 9

States shall separate information systems used by combatants from those used by noncombatants. States shall not use information systems used by noncombatants to shield information systems used by combatants from attack, and shall not embed medical information systems in other military information systems that are lawful objects of attack.

Article 10

States shall launch information attacks from only information systems operated by lawful combatants. States shall not use the information systems of noncombatants or nonparties to the conflict as proxies for such attacks. States shall take reasonable measures to prohibit and prevent such attacks by private persons.

Article 11

States engaging in information attacks shall make best efforts to minimize the adverse effects of information warfare on noncombatants.

Article 12

Information attacks calculated to cause physical damage shall be directed against only targets whose destruction, damage or neutralization confers a definite military advantage, provided that military advantage outweighs the adverse effect on civilians or the civilian population.

Article 13

Information attacks which are intended or may be reasonably expected to cause widespread, long-term, and severe damage to the natural environment, and thereby to prejudice the health or survival of the population, are prohibited.

Article 14

In addition to the prohibitions set forth in Articles 12 and 13 of this Convention, information attacks directed against works and installations containing dangerous forces, such as dams, dikes, and nuclear facilities, whose attack may cause severe losses among the civilian population, shall be attacked only if they are used in regular, significant and direct support of military operations, and if such attack is the only feasible way to terminate such support.

Article 15

Information attacks directed against any of the following facilities shall be prohibited:

a. Medical and religious facilities.

b. Banks; stock, bond and commodities markets; and any other financial institutions.

c. Supplies and distribution systems for food and water, unless the supply or distribution system is used exclusively for providing food and water to lawful combatants.

d. Supplies and distribution systems for electricity and other energy sources for the civilian population, unless the systems are used to supply energy to military installations, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population.

e. Communications systems used by the civilian population, unless the systems are also used by combatant forces, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population.

f. Sites protected as cultural property.

This Convention shall not prejudice the right to attack the above facilities if they are being used to shield other, lawful targets from attack.

Article 16

States shall use all reasonable means to ensure that information attacks involving malicious code, including logic bombs, discriminate between information systems used by combatants and those used by noncombatants and neutral States.

Article 17

States shall program logic bombs to neutralize themselves automatically once they are no longer reasonably anticipated to serve a legitimate military purpose.

III. Rules of Warfare

Article 18

States shall conduct information warfare according to customary international law principles of military necessity, proportionality, humanity, and chivalry. States shall not conduct information attacks in a manner so as to cause superfluous injury or unnecessary suffering.

Article 19

States shall not conduct commercial or financial transactions that are fraudulent or under false pretense as a means of warfare

Article 20

States shall not interfere with the personal finances of any individuals, including combatants and public officials, as a means of warfare. Violations of this article include, but are not limited to, interfering with payroll systems, transferring money or other capital assets without authorization, and altering or erasing records of ownership of money or assets.

Article 21

States shall not engage in identity theft against individuals as a means of warfare, nor shall States obtain and display personal identifiers of individuals, whose display would facilitate identity theft from such individuals by other States or non-State actors.

Article 22

The practice of contacting military members at their residences, for example, by electronic mail, shall not be prohibited. However, States shall engage in such practices in a manner so as not to terrorize noncombatants, including the family members of military members.

Article 23

The use of information systems to invite the confidence of an adversary to lead it to believe that an individual, location, or facility is entitled to protection under the law of armed conflict, with intent to betray that confidence, constitutes perfidy, and States shall be forbidden from engaging in such acts.

Article 24

States shall not transmit malicious code disguised as harmless electronic message traffic if:

a. The message is disguised as originating from an official in the government or armed forces of any State other than the attacking State;

b. The message is disguised as originating from any State other than the attacking State or the target State; or

c. The message is disguised as originating from any medical or religious establishment of or within any State, or any other person or institution of or within any State that is accorded protected status.

Article 25

The alteration of images or recordings shall be prohibited if:

a. The alteration falsely depicts any individual engaged in an unlawful, lewd or lascivious, or sacrilegious act, with the intent to induce others to believe that the individual actually committed the act, when the individual in fact did not commit the act;

b. The alteration falsely depicts a war crime, whether actual or imminent, particularly but not limited to an atrocity or attack on a protected site, with the intent to induce others to believe that another State actually committed the war crime, atrocity, or attack, or is about to do so, when that State in fact did not do so and is not about to do so; or

c. The alteration falsely depicts an attack by another State against any third State with the intent to induce others to believe that such an attack has actually taken place or is imminent, when such an attack in fact has not taken place and is not imminent.

IV. Rights of States Not Party to an Armed Conflict

Article 26

a. Belligerent States shall not engage in information attacks against neutral States.

b. Neutral States shall not actively assist or facilitate information attacks against belligerent States.

Article 27

A State shall not use domain names or information systems for military purposes, or conduct any information warfare activities, within the jurisdiction of any other State, unless it does so with the consent of that other State.

Article 28

Belligerent States shall not launch information attacks from computer systems in neutral States, or take control of such systems in furtherance of information attacks. Belligerent States shall not intentionally route information attacks through neutral States.

Article 29

Computer systems and communications lines in neutral States shall not be the object of attack, physical or otherwise, even if they are used as conduits for an information attack, unless the neutral State is actively assisting an attacking State in committing the attack.

Article 30

A neutral State is not required to sever communications or Internet links with belligerent States. If a belligerent State deliberately violates a neutral State's rights of neutrality, the neutral State shall be permitted to sever communications and Internet links with the violating State, but shall not be required to sever the same links with the other belligerent States. However, if several belligerent States violate the neutral State's neutrality, the neutral State may sever links with the belligerent States in a manner proportional to the severity of the violations, provided that the neutral State treat equivalent violations equally. If the neutral State chooses to sever communications and/or Internet links with any belligerent States without cause, the neutral State must sever the same links with all the belligerent States.

V. Enforcement

Article 31

States shall enact legislation to prohibit noncombatants within its jurisdiction from engaging in information attacks against other States and shall prescribe criminal penalties for the same. States shall take all reasonable and appropriate measures to prevent and punish noncombatants within its jurisdiction from engaging in information attacks against other States.

Article 32

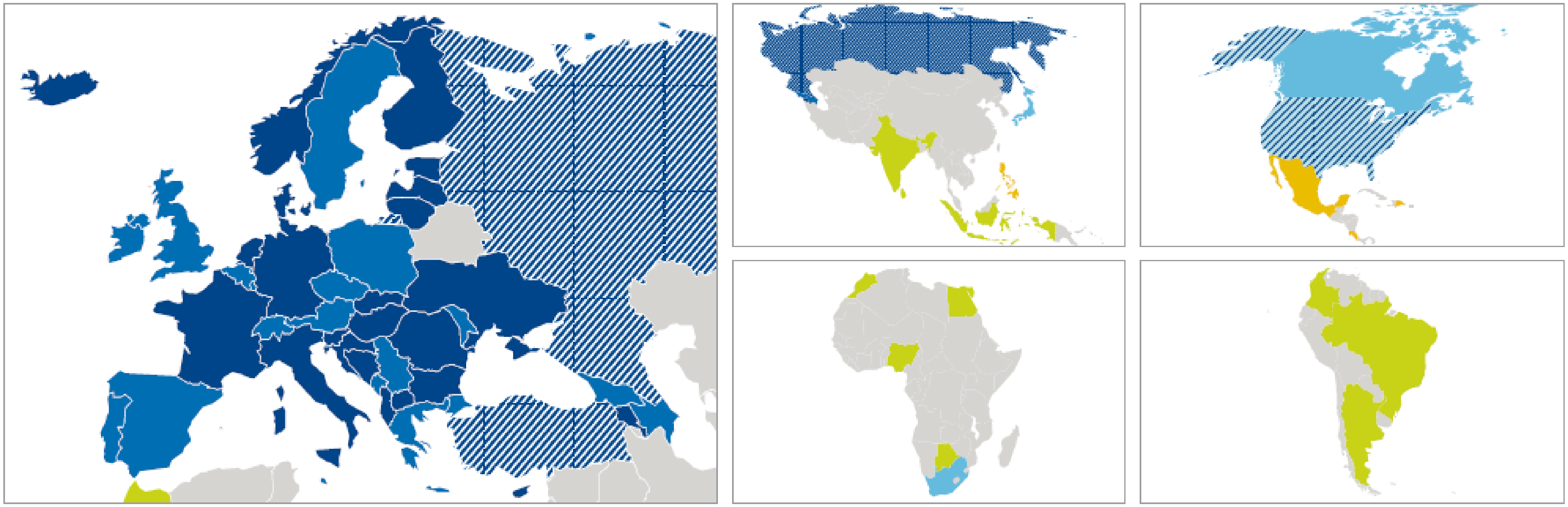
States shall submit disputes and claims arising under this Convention to the International Court of Justice or other adjudicatory bodies as established by the Parties.

VI. Miscellaneous

[amendments, ratification, deposit, entry into force, authentic texts, etc.]
[signatures]

Appendix C

Global reach of the Council of Europe Convention on Cybercrime



Countries party to the Convention

Council of Europe member states

■ Albania
Armenia
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Denmark
Estonia
Finland
France
Germany
Hungary
Iceland
Italy
Latvia
Lithuania
Netherlands
Norway
Romania
Slovak Republic
Slovenia
«the former Yugoslav Republic of Macedonia »
Ukraine

Non Council of Europe member states

▨ United States*

Signatory countries

Council of Europe member states

🟦 Austria
Azerbaijan
Belgium
Czech Republic
Georgia
Greece
Ireland
Liechtenstein
Luxembourg
Malta
Moldova
Montenegro
Poland
Portugal
Serbia
Spain
Sweden
Switzerland
United Kingdom

Non Council of Europe member states

🟦 South Africa
Canada*
Japan*

Countries which did neither ratify nor sign the Convention

Council of Europe member states

▨ Andorra
Monaco
Russia
San Marino
Turkey

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Source: Council of Europe.
9th March 2009

Countries that are known to use the Convention as a guideline for their national legislation

Non Council of Europe member states

🟩 Argentina
Botswana
Brazil
Colombia
Egypt
India
Indonesia
Morocco
Nigeria
Sri Lanka

Non Council of Europe member states invited to accede

🟨 Costa Rica
Dominican Republic
Mexico*
Philippines

* observer countries